Verwaltung von VMware View

View 5.0
View Manager 5.0
View Composer 2.7

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000502-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/pubs/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2011 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter http://www.vmware.com/go/patents-de aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Verwaltung von VMware View 7

1 Konfigurieren von View Connection Server 9
- Verwenden von View Administrator 9
- Konfigurieren von vCenter Server und View Composer 12
- Sichern von View Connection Server 18
- Konfigurieren der Einstellungen für Clientsitzungen 18
- Deaktivieren oder Aktivieren von View Connection Server 23
- Bearbeiten der externen URLs 24
- View LDAP-Verzeichnis 25
- Konfigurieren von View Connection Server-Einstellungen 25

2 Konfigurieren der rollenbasierten Verwaltungsdelegierung 27
- Grundlegendes zu Rollen und Berechtigungen 27
- Verwenden von Ordnern für die Verwaltungsdelegierung 28
- Grundlegendes zu Berechtigungen 29
- Verwalten von Administratoren 30
- Verwalten und Überprüfen von Berechtigungen 32
- Verwalten und Überprüfen von Ordnern 34
- Verwalten von benutzerdefinierten Rollen 36
- Vordefinierte Rollen und Berechtigungen 38
- Erforderliche Berechtigungen für häufige Aufgaben 42
- Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen 45

3 Vorbereiten nicht verwalteter Desktop-Quellen 47
- Vorbereiten einer nicht verwalteten Desktop-Quelle für die View-Desktop-Bereitstellung 47
- Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle 48

4 Erstellen und Vorbereiten virtueller Maschinen 51
- Erstellen virtueller Maschinen für die View-Desktop-Bereitstellung 51
- Installieren von View Agent auf einer virtuellen Maschine 57
- Unbeaufsichtigte Installation von View Agent 59
- Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent 64
- Optimieren der Leistung des Windows-Gastbetriebssystems 65
- Optimieren der Leistung des Windows 7-Gastbetriebssystems 66
- Optimieren von Windows 7 für Linked-Clone-Desktops 66
- Vorbereiten virtueller Maschinen für View Composer 75
- Erstellen von Vorlagen virtueller Maschinen 81
- Erstellen von Anpassungsspezifikationen 81

5 Erstellen von Desktop-Pools 83
Automatisierte Pools mit vollständigen virtuellen Maschinen 84
Pools von Linked-Clone-Desktops 89
Manuelle Desktop-Pools 111
Microsoft-Terminaldienste-Pools 116
Bereitstellen von Desktop-Pools 118
Einstellen von Betriebsrichtlinien für Desktop-Pools 132

6 Berechtigen von Benutzern und Gruppen 139
Hinzufügen von Berechtigungen zu Desktop-Pools 139
Entfernen von Berechtigungen für einen Desktop-Pool 140
Überprüfen von Berechtigungen für Desktop-Pools 140
Einschränken des Zugriffs auf View-Desktops 140

7 Einrichten der Benutzerauthentifizierung 145
Verwenden der Smartcard-Authentifizierung 145
Verwenden der Smartcard-Zertifikatssperrüberprüfung 156
Verwenden der RSA SecurID-Authentifizierung 159
Verwenden der Funktion „Anmelden als aktueller Benutzer“ 162

8 Konfigurieren von Richtlinien 163
Festlegen von Richtlinien in View Administrator 163
Verwenden von Active Directory-Gruppenrichtlinien 168
Verwenden der Gruppenrichtlinien-ADM-Vorlagendateien für View 169
Einrichten des standortbasierten Drucks 200
Verwenden von Terminaldienste-Gruppenrichtlinien 204
Beispiel einer Active Directory-Gruppenrichtlinie 205

9 Konfigurieren von Benutzerprofilen mit View Persona-Verwaltung 211
Bereitstellen von Benutzerpersonas in View 211
Persona-Verwaltung und servergespeicherte Windows-Profile 212
Konfigurieren einer View Persona-Verwaltung-Bereitstellung 212
Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona-Verwaltung-Bereitstellung 220
Gruppenrichtlinieneinstellungen für View Persona-Verwaltung 223

10 Verwalten von Linked-Clone-Desktops 231
Reduzieren der Größe von verknüpften Klonen durch eine Desktop-Aktualisierung 231
Aktualisieren von Linked-Clone-Desktops 233
Neuverteilen von Linked-Clone-Desktops 238
Verwalten persistenter View Composer-Festplatten 241

11 Verwalten von Desktops und Desktop-Pools 247
Verwalten von Desktop-Pools 247
Reduzieren der Adobe Flash-Bandbreite 253
Verwalten von VM-Desktops 255
Exportieren von View-Informationen in externe Dateien 260

12 Verwalten von physischen Computern und Terminalservern 263
Hinzufügen einer nicht verwalteten Desktop-Quelle zu einem Pool 263
Entfernen einer nicht verwalteten Desktop-Quelle aus einem Pool 264
Löschen eines Pools mit nicht verwalteten Desktops 264
Aufheben der Registrierung für eine nicht verwaltete Desktop-Quelle 265
Desktop-Status von physischen Computern und Terminalservern 265

13 Verwalten von ThinApp-Anwendungen in View Administrator 267
View-Anforderungen für ThinApp-Anwendungen 267
Erfassen und Speichern von Anwendungspaketen 268
Zuweisen von ThinApp-Anwendungen zu Desktops und Pools 272
Warten von ThinApp-Anwendungen in View Administrator 279
Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in View Administrator 282
ThinApp-Konfigurationsbeispiel 286

14 Verwalten von lokalen Desktops 289
Vorteile bei der Verwendung von View-Desktops im lokalen Modus 289
Verwalten von View Transfer Server 297
Verwalten des Transfer Server-Repositorys 302
Verwalten von Datenübertragungen 309
Konfigurieren von Sicherheits- und Optimierungseinstellungen für lokale Desktop-Vorgänge 313
Konfigurieren der Ressourcennutzung für Endpunkte 318
Konfigurieren eines HTTP-Caches für die Bereitstellung lokaler Desktops über ein WAN 323
Konfigurieren des Taktsignalintervalls für Clientcomputer mit lokalem Desktop 327
Manuelles Herunterladen eines lokalen Desktops an einem Standort mit unzureichenden Netzwerkverbindungen 328
Fehlerbehebung bei View Transfer Server- und lokalen Desktop-Vorgängen 332

15 Warten von View-Komponenten 343
Sichern und Wiederherstellen von View-Konfigurationsdaten 343
Überwachen von View-Komponenten 349
Überwachen des Desktop-Status 349
Grundlegendes zu den View Manager-Diensten 350
Hinzufügen von Lizenzen zu VMware View 352
Aktualisieren allgemeiner Benutzerinformationen aus Active Directory 353
Migrieren von View Composer mit einer vorhandenen Datenbank 353
Aktualisieren der Zertifikate auf einer View Connection Server-Instanz oder einem Sicherheitsserver 355

16 Fehlerbehebung bei View-Komponenten 357
Überwachen des Systemzustands 358
Überwachen von Ereignissen in View Manager 358
Senden von Nachrichten an Desktop-Benutzer 359
Anzeigen von Desktops, auf denen Probleme vermutet werden 359
Verwalten von Desktops und Richtlinien für nicht berechtigte Benutzer 360
Sammeln von Diagnoseinformationen für VMware View 361
Aktualisieren von Supportanfragen 365
Weitere Informationen zur Fehlerbehebung 365

Fehlerbehebung bei Problemen mit der Netzwerkverbindung 365
Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung 370
Fehlerbehebung bei Problemen mit der USB-Umleitung 373
Beheben von Fehlern bei der QuickPrep-Anpassung 375
View Composer-Bereitstellungsfehler 376
Fehler beim Hinzufügen von verknüpften Windows XP-Klonen zur Domäne 378
Fehlerbehebung von GINA-Problemen auf Windows XP-Desktops 378

17 Verwenden des Befehls „vdmadmin“ 381
Verwendung des Befehls „vdmadmin“ 383
Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“ 385
Außerkraftsetzen von IP-Adressen unter Verwendung der Option „-A“ 387
Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C“ 388
Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“ 388
Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H“ 389
Auflisten und Anzeigen von Berichten zum View Manager-Betrieb unter Verwendung der Option „-I“ 390
Zuweisen von dedizierten Desktops unter Verwendung der Option „-L“ 391
Anzeigen von Informationen zu Maschinen unter Verwendung der Option „-M“ 392
Konfigurieren von Domänenfiltern unter Verwendung der Option „-N“ 393
Konfigurieren von Domänenfiltern 396
Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“ 400
Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q“ 401
Anzeigen des ersten Benutzers eines Desktops unter Verwendung der Option „-R“ 405
Entfernen des Eintrags für eine View Connection Server-Instanz unter Verwendung der Option „-S“ 406
Festlegen einer maximalen Größe für Paketdateien mithilfe der Option „-T“, um View Transfer Server-Pakete bei der Veröffentlichung zu unterteilen 407
Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“ 407
Entschlüsseln der virtuellen Maschine eines lokalen Desktops unter Verwendung der Option „-V“ 408
Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V“ 409
Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“ 410

18 Einrichten von Clients im Kiosk-Modus 413
Konfigurieren von Clients im Kiosk-Modus 414

19 Ausführen von View Client über die Befehlszeile 425
Verwenden von View Client-Befehlen 425
View Client-Konfigurationsdatei 427
View Client-Registrierungseinstellungen 428
View Client-Exitcodes 428

Index 431

Verwaltung von VMware View

Das Handbuch *Verwaltung von VMware View* beschreibt die Konfiguration und Verwaltung von VMware View™. Hierzu zählen u.a. folgende Aufgaben: Konfigurieren von View Connection Server, Erstellen von Administratoren, Provisionieren und Bereitstellen von View-Desktops, Einrichten der Benutzerauthentifizierung, Konfigurieren von Richtlinien und Verwalten von VMware ThinApp™-Anwendungen in View Administrator. Darüber hinaus wird in diesem Handbuch beschrieben, wie Sie VMware View-Komponenten verwalten und eventuell auftretende Probleme beheben.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die VMware View konfigurieren und verwalten möchten. Die bereitgestellten Informationen sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb von Rechenzentren vertraut sind.

Konfigurieren von View Connection Server 1

Nachdem Sie View Connection Server installiert und die Erstkonfiguration durchgeführt haben, können Sie vCenter Server-Instanzen und View Composer-Dienste zu View Manager hinzufügen, Rollen erstellen, um Administratorverantwortlichkeiten zu delegieren, sowie Sicherungen Ihrer Konfigurationsdaten planen.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwenden von View Administrator“, auf Seite 9
- „Konfigurieren von vCenter Server und View Composer“, auf Seite 12
- „Sichern von View Connection Server“, auf Seite 18
- „Konfigurieren der Einstellungen für Clientsitzungen“, auf Seite 18
- „Deaktivieren oder Aktivieren von View Connection Server“, auf Seite 23
- „Bearbeiten der externen URLs“, auf Seite 24
- „View LDAP-Verzeichnis“, auf Seite 25
- „Konfigurieren von View Connection Server-Einstellungen“, auf Seite 25

Verwenden von View Administrator

View Administrator ist die Web-Oberfläche, mit der Sie View Connection Server konfigurieren und Ihre View-Desktops verwalten können.

Einen Vergleich der Vorgänge, die Sie mit View Administrator, View-Cmdlets und `vdmadmin` durchführen können, finden Sie im Dokument *Integration von VMware View*.

View Administrator und View Connection Server

View Administrator stellt eine Verwaltungsschnittstelle für View Manager bereit.

Abhängig von Ihrer View-Bereitstellung können Sie eine oder mehrere View Administrator-Schnittstellen verwenden.

- Verwenden Sie eine View Administrator-Schnittstelle zum Verwalten der View-Komponenten, die mit einer einzelnen, eigenständigen View Connection Server-Instanz oder einer Gruppe replizierter View Connection Server-Instanzen verknüpft sind.

  Sie können die IP-Adresse einer beliebigen replizierten Instanz verwenden, um sich an View Administrator anzumelden.

- Sie müssen eine separate View Administrator-Schnittstelle zum Verwalten der View-Komponenten für jede einzelne, eigenständige View Connection Server-Instanz und jede Gruppe replizierter View Connection Server-Instanzen verwenden.

Sie verwenden View Administrator außerdem zum Verwalten von Sicherheitsservern und View Transfer Server-Instanzen, die mit View Connection Server verknüpft sind.

- Jeder Sicherheitsserver ist mit einer View Connection Server-Instanz verknüpft.
- Jede View Transfer Server-Instanz kann mit einer beliebigen View Connection Server-Instanz in einer Gruppe replizierter Instanzen kommunizieren.

Anmelden an View Administrator

Zum Ausführen anfänglicher Konfigurationsaufgaben müssen Sie sich an View Administrator anmelden.

Voraussetzungen

- Stellen Sie sicher, dass View Connection Server auf einem dedizierten Computer installiert ist.
- Vergewissern Sie sich, dass Sie einen von View Administrator unterstützten Webbrowser verwenden. Informationen zu den View Administrator-Anforderungen finden Sie im Dokument *Installation von VMware View*.

Vorgehensweise

1 Öffnen Sie Ihren Webbrowser und geben Sie die folgende URL ein. Hierbei steht *Server* für den Hostnamen oder die IP-Adresse der View Connection Server-Instanz:

```
https://Server/admin
```

Sie können unter Verwendung einer sicheren Verbindung (SSL) auf View Administrator zugreifen. Bei der ersten Verbindungsherstellung zeigt Ihr Webbrowser möglicherweise eine Warnung an, nach der das mit der Adresse verknüpfte Sicherheitszertifikat nicht durch eine vertrauenswürdige Zertifizierungsstelle ausgegeben wurde. Dieses Verhalten ist normal, da es sich bei dem zum Lieferumfang von View Connection Server gehörenden Standardzertifikat um ein selbst signiertes Zertifikat handelt.

2 Klicken Sie auf **[Ignore (Ignorieren)]** , um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren.

3 Melden Sie sich mit Administratoranmeldeinformationen am View Connection Server-Computer an.

Anfänglich sind alle Benutzer, die Mitglieder der lokalen Administratorengruppe (BUILTIN\Administrators) auf dem View Connection Server-Computer sind, zur Anmeldung an View Administrator berechtigt.

Nach der Anmeldung an View Administrator können Sie **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** verwenden, um die Liste der Benutzer und Gruppen zu ändern, die Administratorrolle für View haben.

Tipps zur Verwendung der View Administrator-Oberfläche

Sie können mithilfe der View Administrator-Benutzeroberflächenfunktionen in View-Seiten navigieren, nach View-Objekten suchen sowie View-Objekte filtern und sortieren.

View Administrator umfasst viele gängige Benutzeroberflächenfunktionen. So werden Sie z.B. im linken Navigationsbereich auf jeder Seite auf weitere View Administrator-Seiten weitergeleitet. Mit den Suchfiltern können Sie Filterkriterien in Bezug auf die gesuchten Objekte auswählen.

Tabelle 1-1 werden einige weitere Funktionen beschrieben, die die Verwendung von View Administrator unterstützen.

Tabelle 1-1. View Administrator-Navigations- und Anzeigefunktionen

View Administrator-Funktion	Beschreibung
In View Administrator-Seiten rückwärts und vorwärts navigieren.	Klicken Sie auf die Schaltfläche **[Back (Zurück)]** im oberen linken Bereich einer View Administrator-Seite, um zur zuvor angezeigten View Administrator-Seite zu wechseln. Klicken Sie auf die Schaltfläche **[Forward (Weiter)]** , um zur aktuellen Seite zurückzukehren. Verwenden Sie nicht die Schaltfläche **[Back (Zurück)]** Ihres Browsers. Mit dieser Schaltfläche wird die Anmeldeseite von View Administrator angezeigt.
Mehrspaltige Sortierung	Sie können View-Objekte mithilfe der mehrspaltigen Sortierung auf unterschiedliche Art und Weise sortieren. Klicken Sie auf eine Überschrift in der obersten Zeile einer View Administrator-Tabelle, um die View-Objekte alphabetisch anhand dieser Überschrift zu sortieren. Beispielsweise können Sie auf der Seite **[Inventory (Bestandsliste)] > [Desktops]** auf **[Pool]** klicken, um Desktops nach den Pools zu sortieren, die sie enthalten. Neben der Überschrift wird die Zahl **[1]** angezeigt, um anzugeben, dass sie die Spalte für die primäre Sortierung ist. Sie können erneut auf die Überschrift klicken, um die Sortierreihenfolge umzukehren. Dies wird durch einen nach oben oder unten weisenden Pfeil angezeigt. Um die View-Objekte nach einem zweiten Element zu sortieren, markieren Sie eine weitere Überschrift mit der Tastenkombination Strg+Klick. Sie können z.B. in der Tabelle **[Desktops]** auf **[Users (Benutzer)]** klicken, um eine zweite Sortierung nach den Benutzern durchzuführen, denen die Desktops zugeordnet sind. Neben der zweiten Überschrift wird die Zahl **[2]** angezeigt. In diesem Beispiel werden die Desktops nach dem Pool und nach den Benutzern in jedem Pool sortiert. Sie können mit Strg+Klick alle Spalten in einer Tabelle in absteigender Reihenfolge ihrer Bedeutung sortieren. Drücken Sie Strg+Umschalt+Klick, um die Auswahl eines Sortierelements aufzuheben. Sie möchten z.B. die Desktops in einem Pool anzeigen, die sich in einem bestimmten Zustand befinden und in einem bestimmten Datenspeicher gespeichert sind. Klicken Sie auf **[Inventory (Bestandsliste)] > [Pools]** und dann auf die Pool-ID. Klicken Sie anschließend auf die Überschrift **[Datastore (Datenspeicher)]** und drücken Sie Strg+Klick in der Überschrift **[Status]** .
Auswählen von View-Objekten und Anzeigen von View-Objektdetails	Sie können in View Administrator-Tabellen, die View-Objekte auflisten, ein Objekt auswählen oder Objektdetails anzeigen. ■ Um ein Objekt auszuwählen, klicken Sie in der Tabelle in der Objektzeile auf eine beliebige Stelle. Im oberen Bereich der Seite werden die Menüs und Befehle, die das Objekt verwalten, aktiv. ■ Um Objektdetails anzuzeigen, doppelklicken Sie in der Objektzeile auf die linke Zelle. Es wird eine neue Seite in den Objektdetails angezeigt. Klicken Sie beispielsweise auf der Seite **[Inventory (Bestandsliste)] > [Pools]** auf eine beliebige Stelle in der Zeile eines bestimmten Pools, um die Befehle zu diesem Pool zu aktivieren. Doppelklicken Sie auf die Zelle **[Pool ID (Pool-ID)]** in der linken Spalte, um eine neue Seite anzuzeigen, die Details zum Pool enthält.
Erweitern von Dialogfeldern zur Anzeige von Detailinformationen	Sie können View Administrator-Dialogfelder erweitern, um Detailinformationen wie z.B. Desktop-Namen und Benutzernamen in Tabellenspalten anzuzeigen. Zum Erweitern eines Dialogfelds platzieren Sie die Maus über den Punkten in der rechten unteren Ecke des Dialogfelds und führen Sie eine Ziehoperation aus.

Fehlerbehebung bei Zugriffsproblemen auf View Administrator ohne eine sichere SSL-Verbindung

Sie können sich nicht über einen Webbrowser an View Administrator anmelden, wenn die SSL-Einstellung für Ihre View-Clients nicht mit der URL übereinstimmt, die Sie für die Verbindung mit View Administrator verwenden. Wenn Sie die SSL-Einstellung deaktivieren, ist eine Verwendung von **`https`** in der URL nicht möglich.

Problem

Die URL, die Sie zum Anmelden an View Administrator verwenden, funktioniert nicht mehr. Ein Verbindungsfehler ist aufgetreten.

Ursache

View Manager verwendet standardmäßig SSL, um sichere Verbindungen zwischen View-Clients und View Connection Server herzustellen. Diese Einstellung wird auch auf Computern angewendet, die über einen Webbrowser mit View Administrator verbunden sind.

Dieses Problem tritt auf, wenn Sie diese Einstellung in View Administrator ändern, indem Sie zu **[View Configuration (View-Konfiguration)] > [Global Settings (Globale Einstellungen)]** wechseln und das Kontrollkästchen **[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]** deaktivieren.

Lösung

Verwenden Sie die folgende URL für die Verbindung zu View Administrator, wobei *Server* der Hostname oder die IP-Adresse der View Connection Server-Instanz ist.

`http://`*`Server`*`/admin`

Fehlerbehebung bei der Textanzeige in View Administrator

Wenn Ihr Webbrowser auf einem Nicht-Windows-Betriebssystem wie beispielsweise Linux, UNIX oder Mac OS ausgeführt wird, wird der Text in View Administrator nicht ordnungsgemäß angezeigt.

Problem

Der Text in der View Administrator-Oberfläche ist unleserlich. Es treten beispielsweise Leerzeichen in Wörtern auf.

Ursache

Für View Administrator sind Microsoft-spezifische Schriftarten erforderlich.

Lösung

Installieren Sie Microsoft-spezifische Schriftarten auf Ihrem Computer.

Derzeit werden auf der Microsoft-Website keine Microsoft-Schriftarten bereitgestellt, Sie können die Schriftarten jedoch von unabhängigen Websites herunterladen.

Konfigurieren von vCenter Server und View Composer

Sie müssen zum Verwenden von virtuellen Maschinen als Desktop-Quellen View Manager konfigurieren, um mit vCenter Server zu kommunizieren. Um Linked-Clone-Desktops zu erstellen und zu verwalten, müssen Sie die View Composer-Einstellungen in View Manager konfigurieren.

Hinzufügen von vCenter Server-Instanzen zu View Manager

Sie müssen View Manager zur Verbindungsherstellung mit den vCenter Server-Instanzen in Ihrer View-Bereitstellung konfigurieren. vCenter Server erstellt und verwaltet die virtuellen Maschinen, die View Manager als Desktop-Quellen verwendet.

Wenn Sie vCenter Server-Instanzen in einer Linked Mode-Gruppe ausführen, muss jede vCenter Server-Instanz separat zu View Manager hinzugefügt werden.

Voraussetzungen

- Installieren Sie den View Connection Server-Produktlizenzschlüssel.
- Erstellen Sie einen vCenter Server-Benutzer mit Berechtigungen zum Ausführen der Vorgänge in vCenter Server, die zur Unterstützung von View Manager erforderlich sind. Wenn Sie View Composer verwenden, müssen Sie dem Benutzer zusätzliche Berechtigungen gewähren. Zur Verwaltung von Desktops, die im lokalen Modus verwendet werden, müssen Sie dem Benutzer zusätzliche Berechtigungen zu den erforderlichen Berechtigungen für View Manager und View Composer erteilen.

  Weitere Informationen zum Konfigurieren eines vCenter Server-Benutzers für View Manager finden Sie im Dokument *Installation von VMware View*.
- Wenn View Connection Server über eine sichere Verbindung (SSL) mit der vCenter Server-Instanz verbunden werden soll, installieren Sie ein SSL-Serverzertifikat auf dem vCenter Server-Host.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Klicken Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** auf **[Add (Hinzufügen)]** .

3 Geben Sie im Textfeld für die Serveradresse den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der vCenter Server-Instanz ein.

  Der FQDN umfasst den Hostnamen und den Domänennamen. Beispiel: Beim vollqualifizierten Domänennamen ***myserverhost.companydomain*.com** ist ***myserverhost*** der Hostname und ***companydomain*.com** die Domäne.

  HINWEIS Wenn Sie einen Server unter Verwendung eines DNS-Namens oder einer URL angeben, führt View Manager kein DNS-Lookup durch um zu überprüfen, ob der Server zuvor unter Verwendung seiner IP-Adresse eingegeben wurde. Es entsteht ein Konflikt, wenn eine vCenter Server-Instanz sowohl mit dem DNS-Namen als auch mit der IP-Adresse angegeben wird.

4 Geben Sie den Namen des vCenter Server-Benutzers ein.

5 Geben Sie das Kennwort für den vCenter Server-Benutzer ein.

6 (Optional) Geben Sie eine Beschreibung für diese vCenter Server-Instanz ein.

7 Um sich über eine sichere Verbindung (SSL) mit der vCenter Server-Instanz zu verbinden, müssen Sie die Option **[Connect using SSL (Verbindung über SSL)]** aktivieren. Die Verwendung einer SSL-Verbindung ist die Standardeinstellung.

8 Geben Sie die TCP-Portnummer ein.

  Der standardmäßige Port lautet 443.

9 (Optional) Klicken Sie auf **[Advanced (Erweitert)]** , um die maximale Anzahl gleichzeitiger Pool-Vorgänge in vCenter Server zu konfigurieren.

a Legen Sie die maximale Anzahl gleichzeitiger Bereitstellungsvorgänge fest.

Diese Einstellung legt die maximale Anzahl gleichzeitiger Anforderungen fest, die View Manager zur Bereitstellung vollständiger virtueller Maschinen in dieser vCenter Server-Instanz senden kann. Der Standardwert lautet acht. Diese Einstellung steuert nicht die Linked-Clone-Bereitstellung.

b Legen Sie die maximale Anzahl gleichzeitiger Betriebsvorgänge fest.

Diese Einstellung legt die maximale Anzahl an Betriebsvorgängen (Start, Herunterfahren, Anhalten usw.) fest, die gleichzeitig auf virtuellen Maschinen ausgeführt werden können, die in dieser vCenter Server-Instanz von View Manager verwaltet werden. Der Standardwert lautet fünf. Diese Einstellung steuert die Betriebsvorgänge vollständiger virtueller Maschinen und verknüpfter Klone.

10 Wählen Sie, ob View Composer konfiguriert werden soll.

Option	Aktion
Sie verwenden View Composer nicht	Klicken Sie auf **[OK]** .
Sie verwenden View Composer	Konfigurieren Sie die View Composer-Einstellungen.

Weiter

Wenn diese View Connection Server-Instanz oder Gruppe replizierter View Connection Server-Instanzen mehrere vCenter Server-Instanzen verwendet, wiederholen Sie diesen Vorgang, um die weiteren vCenter Server-Instanzen hinzuzufügen.

Entfernen einer vCenter Server-Instanz aus View Manager

Sie können die Verbindung zwischen View Manager und einer vCenter Server-Instanz entfernen. Dann werden in View Manager die View-Desktops, die in dieser vCenter Server-Instanz erstellt wurden, nicht mehr verwaltet.

Voraussetzungen

Löschen Sie alle View-Desktops, die mit der vCenter Server-Instanz verknüpft sind. Siehe „Löschen eines Desktop-Pools aus View Manager“, auf Seite 252.

Vorgehensweise

1 Klicken Sie auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** die vCenter Server-Instanz aus.

3 Klicken Sie auf **[Remove (Entfernen)]** .

Sie werden über ein Dialogfeld gewarnt, dass View Manager über keinen Zugriff auf die virtuellen Maschinen mehr verfügt, die von dieser vCenter Server-Instanz verwaltet werden.

4 Klicken Sie auf **[OK]** .

View Manager kann nicht länger auf die virtuellen Maschinen zugreifen, die in der vCenter Server-Instanz erstellt wurden.

Erstellen eines Benutzerkontos für View Composer

Wenn Sie View Composer verwenden, müssen Sie in Active Directory ein Benutzerkonto zur Verwendung mit View Composer erstellen. Dieses Konto ist für View Composer erforderlich, um Linked-Clone-Desktops zur Active Directory-Domäne hinzuzufügen.

Zur Gewährleistung der Sicherheit sollten Sie ein separates Benutzerkonto für View Composer erstellen. Durch das Erstellen eines separaten Kontos können Sie sicherstellen, dass keine zusätzlichen Berechtigungen für andere Zwecke gewährt werden. Sie können diesem Konto die Mindestberechtigungen erteilen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind für das View Composer-Konto nicht die Berechtigungen eines Domänenadministrators erforderlich.

Vorgehensweise

1 Erstellen Sie in Active Directory ein Benutzerkonto, das sich in derselben Domäne wie Ihr View Connection Server-Host oder in einer vertrauenswürdigen Domäne befindet.

2 Fügen Sie die Berechtigungen **[Create Computer Objects (Computerobjekte erstellen)]**, **[Delete Computer Objects (Computerobjekte löschen)]** und **[Write All Properties (Alle Eigenschaften schreiben)]** für das Konto in dem Active Directory-Container hinzu, in dem die Linked-Clone-Computerkonten erstellt werden bzw. in den die Linked-Clone-Computerkonten verschoben werden sollen.

   Die folgende Liste zeigt alle für das Benutzerkonto erforderlichen Berechtigungen, einschließlich der standardmäßig zugewiesenen Berechtigungen:

   - List Contents (Inhalt auflisten)
   - Read All Properties (Alle Eigenschaften lesen)
   - Write All Properties (Alle Eigenschaften schreiben)
   - Read Permissions (Berechtigungen lesen)
   - Create Computer Objects (Computerobjekte erstellen)
   - Delete Computer Objects (Computerobjekte löschen)

3 Stellen Sie sicher, dass die Berechtigungen für das Benutzerkonto für den Active Directory-Container und alle untergeordneten Objekte des Containers gelten.

Weiter

Geben Sie das Konto in View Administrator an, wenn Sie View Composer für vCenter Server konfigurieren und Linked-Clone-Desktop-Pools konfigurieren und bereitstellen.

Konfigurieren von View Composer-Einstellungen für vCenter Server

Zur Verwendung von View Composer müssen Sie View Manager mit anfänglichen Einstellungen konfigurieren, die den Einstellungen für den View Composer-Dienst entsprechen, der in vCenter Server installiert ist. View Composer ist eine Funktion von View Manager, der zugehörige Dienst wird jedoch direkt auf virtuellen Maschinen in vCenter Server ausgeführt.

HINWEIS Wenn Sie View Composer nicht verwenden, können Sie diese Aufgabe überspringen.

Voraussetzungen

- Stellen Sie sicher, dass Sie in Active Directory einen Benutzer erstellt haben, der über die Berechtigung zum Hinzufügen und Entfernen virtueller Maschinen zur Active Directory-Domäne bzw. aus der Active Directory-Domäne verfügt, die Ihre verknüpften Klone enthält. Siehe „Erstellen eines Benutzerkontos für View Composer“, auf Seite 15.

- Vergewissern Sie sich, dass View Manager zur Verbindungsherstellung mit vCenter Server konfiguriert wurde. Siehe „Hinzufügen von vCenter Server-Instanzen zu View Manager“, auf Seite 13.

Vorgehensweise

1 Öffnen Sie in View Administrator das Dialogfeld **[Edit vCenter Server (vCenter Server bearbeiten)]** .

   a Klicken Sie auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

   b Wählen Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** den Eintrag für vCenter Server.

   c Klicken Sie auf **[Edit (Bearbeiten)]** .

2 Wählen Sie die Option **[Enable View Composer (View Composer aktivieren)]** aus und stellen Sie sicher, dass die Portnummer mit derjenigen übereinstimmt, die Sie beim Installieren des View Composer-Dienstes in vCenter Server angegeben haben.

   View Manager überprüft, ob der View Composer-Dienst auf der vCenter Server-Instanz ausgeführt wird.

3 Klicken Sie auf **[Add (Hinzufügen)]** , um die Kontoinformationen für den Domänenbenutzer für View Composer hinzuzufügen.

   a Geben Sie den Domänennamen der Active Directory-Domäne ein.

      Beispiel: `domain.com`

   b Geben Sie den Domänenbenutzernamen ein, einschließlich des Domänennamens.

      Beispiel: `domain.com\admin`

   c Geben Sie das Kontokennwort ein.

   d Klicken Sie auf **[OK]** .

   e Um Domänenbenutzerkonten mit Berechtigungen in weiteren Active Directory-Domänen hinzuzufügen, in denen Sie Linked-Clone-Pools bereitgestellt haben, wiederholen Sie die vorangehenden Schritte.

4 Klicken Sie auf **[OK]** , um das Dialogfeld **[Edit vCenter Server (vCenter Server bearbeiten)]** zu schließen.

Weiter

Wiederholen Sie diesen Vorgang für jede vCenter Server-Instanz, in der View Composer-Dienste installiert sind.

Entfernen von View Composer aus View Manager

Sie können die Verbindung zwischen View Manager und dem View Composer-Dienst entfernen, der in einer vCenter Server-Instanz installiert ist. Dann werden in View Manager die Linked-Clone-Desktops, die von View Composer in der vCenter Server-Instanz erstellt wurden, nicht mehr verwaltet.

Bevor Sie die Verbindung mit View Composer deaktivieren, müssen Sie alle Linked-Clone-Desktops, die über View Composer erstellt wurden, aus View Manager entfernen. Nachdem die Verbindung mit View Composer deaktiviert wurde, kann View Manager die verknüpften Klone weder bereitstellen noch verwalten oder löschen. Das Löschen der verknüpften Klone wird nicht durch View Manager erzwungen. Sie müssen diese Aufgabe eigenständig ausführen.

Vorgehensweise

1 Entfernen Sie die Linked-Clone-Pools, die von View Composer erstellt wurden.

   a Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

   b Wählen Sie einen Linked-Clone-Pool aus und klicken Sie auf **[Delete (Löschen)]** .

   Sie werden über ein Dialogfeld gewarnt, dass Sie den Linked-Clone-Pool aus View Manager endgültig löschen. Die virtuellen Maschinen werden aus vCenter Server gelöscht. Die dazugehörigen View Composer-Datenbankeinträge und die Replikate, die von View Composer erstellt wurden, werden auch entfernt.

   c Klicken Sie auf **[OK]** .

   d Wiederholen Sie diese Schritte für jeden Linked-Clone-Pool, der von View Composer erstellt wurde.

2 Klicken Sie auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

3 Wählen Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** die vCenter Server-Instanz aus, in der View Composer installiert ist.

4 Klicken Sie auf **[Edit (Bearbeiten)]** .

5 Deaktivieren Sie im Fensterbereich **[View Composer Settings (View Composer-Einstellungen)]** die Option **[Enable View Composer (View Composer aktivieren)]** und klicken Sie auf **[OK]** .

In dieser vCenter Server-Instanz können Sie keine Linked-Clone-Desktops mehr erstellen, es ist jedoch weiterhin möglich, in der vCenter Server-Instanz vollständige VM-Desktop-Pools zu erstellen und zu verwalten.

Wenn Linked-Clone-Desktops nicht gelöscht wurden, bevor Sie die Verbindung mit View Composer deaktiviert haben, können Sie versuchen, die Verbindung mit View Composer zu aktivieren, die verknüpften Klone zu löschen und die Verbindung mit View Composer wieder zu deaktivieren. Ausführliche Informationen zum Aktivieren von View Composer finden Sie unter „Konfigurieren von View Composer-Einstellungen für vCenter Server“, auf Seite 15.

Konflikte bei eindeutigen IDs für vCenter Server

Wenn Sie mehrere vCenter Server-Instanzen in Ihrer Umgebung konfiguriert haben, kann das Hinzufügen einer neuen Instanz aufgrund von Konflikten bei eindeutigen IDs fehlschlagen.

Problem

Sie versuchen eine vCenter Server-Instanz zu View Manager hinzuzufügen, die eindeutige ID der neuen vCenter Server-Instanz erzeugt jedoch einen Konflikt mit einer vorhandenen Instanz.

Ursache

Zwei vCenter Server-Instanzen können nicht dieselbe eindeutige ID verwenden. Standardmäßig wird die eindeutige vCenter Server-ID zufällig generiert, Sie können die ID jedoch bearbeiten.

Lösung

1 Klicken Sie in vSphere Client auf **[Administration (Verwaltung)]** > **[vCenter Server Settings (vCenter Server-Einstellungen)]** > **[Runtime Settings (Laufzeiteinstellungen)]** .

2 Geben Sie eine neue eindeutige ID ein und klicken Sie auf **[OK]** .

   Details zum Bearbeiten von eindeutigen vCenter Server-IDs finden Sie in der Dokumentation zu vSphere.

Sichern von View Connection Server

Nachdem Sie die anfängliche Konfiguration von View Connection Server abgeschlossen haben, sollten Sie regelmäßige Sicherungen Ihrer View Manager- und View Composer-Konfigurationsdaten planen.

Informationen zum Sichern und Wiederherstellen Ihrer View-Konfiguration finden Sie unter „Sichern und Wiederherstellen von View-Konfigurationsdaten“, auf Seite 343.

Konfigurieren der Einstellungen für Clientsitzungen

Sie können globale Einstellungen für die Clientsitzungen konfigurieren, die von einer View Connection Server-Instanz oder replizierten Gruppe verwaltet werden. Sie können die Dauer bis zur Zeitüberschreitung festlegen, die Verwendung von SSL für Clientverbindungen und View Administrator als erforderlich festlegen, Prä-Anmelde- und Warnmeldungen anzeigen sowie weitere Clientverbindungsoptionen festlegen.

Festlegen von Optionen für Clientsitzungen und -verbindungen

Sie können globale Einstellungen konfigurieren, um festzulegen, wie die Clientsitzungen und -verbindungen funktionieren sollen.

Die globalen Einstellungen sind keiner einzelnen View Connection Server-Instanz zugeordnet. Sie wirken sich auf alle Clientsitzungen aus, die von einer eigenständigen View Connection Server-Instanz oder einer Gruppe von replizierten Instanzen verwaltet werden.

Sie können View Connection Server-Instanzen auch so konfigurieren, dass direkte, nicht getunnelte Verbindungen zwischen View-Clients und View-Desktops verwendet werden. Siehe „Konfigurieren einer sicheren Tunnelverbindung und eines PCoIP Secure Gateways“, auf Seite 21 für Informationen über die Konfiguration direkter Verbindungen.

Voraussetzungen

Machen Sie sich mit den globalen Einstellungen vertraut. Siehe „Globale Einstellungen für Clientsitzungen und -verbindungen“, auf Seite 19.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Global Settings (Globale Einstellungen)]** .

2 Klicken Sie auf **[Edit (Bearbeiten)]** .

3 Konfigurieren Sie die globalen Einstellungen.

4 Klicken Sie auf **[OK]** .

Weiter

Wenn Sie die Einstellung **[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]** ändern, müssen Sie den View Connection Server-Dienst neu starten, damit die Änderungen wirksam werden. In einer Gruppe replizierter View Connection Server-Instanzen müssen Sie den View Connection Server-Dienst auf allen Instanzen in der Gruppe neu starten. Der Windows Server-Computer, auf dem View Connection Server installiert ist, muss nicht neu gestartet werden.

Globale Einstellungen für Clientsitzungen und -verbindungen

Globale Einstellungen legen die Dauer bis zur Zeitüberschreitung für eine Sitzung fest und geben an, ob SSL verwendet wird, ob Clients nach Unterbrechungen erneut authentifiziert werden, View-Komponenten eine sichere interne Kommunikation verwenden, Prä-Anmelde- und Warnmeldungen angezeigt werden und eine einmalige Anmeldung (Single Sign-On, SSO) für lokale Desktop-Vorgänge verwendet wird.

Tabelle 1-2. Globale Einstellungen für Clientsitzungen und -verbindungen

Einstellung	Beschreibung
[Session timeout (Zeitüberschreitung der Sitzung)]	Legt fest, wie lange ein Benutzer eine Sitzung geöffnet lassen kann, nachdem er sich an View Connection Server angemeldet hat. Der Wert wird in Minuten festgelegt. Sie müssen einen Wert eingeben. Der Standardwert lautet 600 Minuten. Wenn für eine Desktop-Sitzung eine Zeitüberschreitung auftritt, wird die Sitzung beendet und die View Client-Instanz wird vom Desktop getrennt.
[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]	Legt fest, ob ein sicherer SSL-Kommunikationskanal zwischen View Connection Server und View-Desktop-Clients sowie zwischen View Connection Server und Clients mit Zugriff auf View Administrator verwendet wird. Wenn Sie diese Einstellung auswählen, müssen Clients SSL-Verbindungen verwenden. Sie müssen diese Einstellung auswählen, wenn Sie die Smartcard-Authentifizierung verwenden. Nachdem Sie diese Einstellung geändert haben, müssen Sie den View Connection Server-Dienst neu starten, damit Ihre Änderung wirksam wird. In einer Gruppe von replizierten View Connection Server-Instanzen müssen Sie jede Instanz neu starten, damit die Änderung übernommen wird.
[Reauthenticate Secure tunnel connections after network interruption (Sichere Tunnelverbindungen nach Netzwerkunterbrechung neu authentifizieren)]	Legt fest, ob die Benutzeranmeldeinformationen nach einer Netzwerkunterbrechung neu authentifiziert werden müssen, wenn View Client-Instanzen sichere Tunnelverbindungen zu View-Desktops verwenden. Wenn bei Auswahl dieser Einstellung während einer Desktop-Sitzung eine sichere Tunnelverbindung abläuft, fordert View Client den Benutzer zur erneuten Authentifizierung auf, bevor die Verbindung wiederhergestellt wird. Ist diese Einstellung nicht ausgewählt, stellt der Client die Verbindung mit dem Desktop wieder her, ohne den Benutzer zur erneuten Authentifizierung aufzufordern. Diese Einstellung bleibt wirkungslos, wenn eine direkte Verbindung verwendet wird.
[Message security mode (Sicherheitsmodus für Nachrichten)]	Legt die Sicherheit der Kommunikation zwischen den View Manager-Komponenten fest. Legt insbesondere fest, ob zwischen den View Manager-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden. Weitere Informationen finden Sie unter „Sicherheitsmodus für Nachrichten für View-Komponenten“, auf Seite 20.
[Disable Single Sign-On for Local Mode operations (SSO für Vorgänge im lokalen Modus deaktivieren)]	Legt fest, ob die einmalige Anwendung aktiviert ist, wenn Benutzer sich an ihren lokalen Desktops anmelden. Wenn Sie diese Einstellung deaktivieren, müssen Benutzer sich manuell an ihren Desktops anmelden, um nach der Anmeldung ihre Windows-Sitzungen zu starten. Wenn Sie diese Einstellung ändern, wird die Änderung für jeden Benutzer beim nächsten Benutzervorgang wirksam.

Tabelle 1-2. Globale Einstellungen für Clientsitzungen und -verbindungen (Fortsetzung)

Einstellung	Beschreibung
[Enable automatic status updates (Automatische Status-Updates aktivieren)]	Legt fest, ob View Manager die globale Statusanzeige im oberen linken Bereich von View Administrator wird mit einem Intervall von wenigen Minuten aktualisiert. Die Dashboard-Seite von View Administrator wird ebenfalls mit einem Intervall von wenigen Minuten aktualisiert. Wenn Sie diese Einstellung aktivieren, wird für im Leerlauf befindliche Sitzungen aller Benutzer, die an View Administrator angemeldet sind, keine Zeitüberschreitung ausgelöst. **Wichtig** Das Deaktivieren von Zeitüberschreitungen für im Leerlauf befindliche Sitzungen erhöht das Risiko einer nicht autorisierten Verwendung von View Administrator. Aktivieren Sie diese Einstellung mit Bedacht. Diese Einstellung ist standardmäßig nicht aktiviert. Für im Leerlauf befindliche Sitzungen werden Zeitüberschreitungen ausgelöst.
[Display a pre-login message (Meldung vor der Anmeldung anzeigen)]	Zeigt View Client-Benutzern bei der Anmeldung einen Haftungsausschluss oder eine andere Meldung an. Geben Sie Ihre Informationen oder Anweisungen in das Textfeld im Dialogfeld **[Global Settings (Globale Einstellungen)]** ein. Wenn keine Meldung angezeigt werden soll, lassen Sie das Textfeld leer.
[Display a warning before forced logoff (Vor erzwungener Abmeldung eine Warnung anzeigen)]	Zeigt eine Warnmeldung an, wenn eine Benutzerabmeldung aufgrund einer geplanten oder sofortigen Aktualisierung erzwungen wird, z.B. beim Start einer Desktop-Aktualisierung. Mit dieser Einstellung wird auch festgelegt, wie lange nach dem Anzeigen der Meldung gewartet wird, bis der Benutzer abgemeldet wird. Aktivieren Sie das Kontrollkästchen, um eine Warnmeldung anzuzeigen. Geben Sie die Anzahl der Minuten ein, die nach der Anzeige der Meldung und vor dem Abmelden des Benutzers abgewartet werden sollen. Der Standardwert lautet 5 Minuten. Geben Sie Ihre Warnmeldung ein. Sie können die Standardmeldung verwenden: `Your desktop is scheduled for an important update and will be restarted in 5 minutes. Please save any unsaved work now. (Für Ihren Desktop wurde eine wichtige Aktualisierung geplant. Ihr Desktop wird in 5 Minuten neu gestartet. Speichern Sie jetzt alle noch nicht gespeicherten Arbeiten.)`

Sicherheitsmodus für Nachrichten für View-Komponenten

Sie können die Sicherheitsebene für die Kommunikation zwischen View-Komponenten festlegen. Mit dieser Einstellung wird festgelegt, ob zwischen View Manager-Komponenten übermittelte JMS-Nachrichten signiert und überprüft werden sollen. Mit dieser Einstellung wird die Verarbeitung von Steuerungsmeldungen verhindert, die nicht von einer autorisierten Quelle stammen.

Neben der Nutzung zur Signierung und Überprüfung von Nachrichten wird als Vorgehensweise empfohlen, IPSec zur Verschlüsselung von Nachrichten zwischen View Connection Sever-Instanzen und zwischen View Connection Sever-Instanzen und Sicherheitsservern zu verwenden.

Wenn eine der Komponenten in Ihrer View-Umgebung eine Version vor View Manager 3.0 verwendet, ist das Signieren und Überprüfen nicht möglich.

Tabelle 1-3 werden die Optionen dargestellt, die Sie zum Konfigurieren der Sicherheitsstufe für Nachrichten auswählen können. Um eine Option festzulegen, wählen Sie die gewünschte Einstellung in der Liste **[Message security mode (Sicherheitsmodus für Nachrichten)]** im Dialogfeld **[Global Settings (Globale Einstellungen)]** aus.

Tabelle 1-3. Optionen für den Sicherheitsmodus für Nachrichten

Option	Beschreibung
[Disabled (Deaktiviert)]	Der Sicherheitsmodus für Nachrichten ist deaktiviert.
[Mixed (Gemischt)]	Der Sicherheitsmodus für Nachrichten ist aktiviert, wird aber nicht erzwungen. Sie können diesen Modus verwenden, um Komponenten in Ihrer View-Umgebung zu ermitteln, die eine Version vor View Manager 3.0 verwenden. Die von View Connection Server generierten Protokolldateien enthalten Verweise auf diese Komponenten.
[Enabled (Aktiviert)]	Der Sicherheitsmodus für Nachrichten ist aktiviert. Nicht signierte Nachrichten werden von View-Komponenten abgelehnt. **Hinweis** View-Komponenten, die eine Version vor View Manager 3.0 verwenden, dürfen mit anderen View-Komponenten nicht kommunizieren.

Der Sicherheitsmodus für Nachrichten wird in View Manager 3.0 und höher unterstützt. Wenn Sie den Sicherheitsmodus für Nachrichten von **[Disabled (Deaktiviert)]** oder **[Mixed (Gemischt)]** auf **[Enabled (Aktiviert)]** setzen, können Sie keinen Desktop starten, der über einen View Agent aus der Virtual Desktop Manager-Version 2.1 oder früher verfügt. Wenn Sie den Sicherheitsmodus für Nachrichten dann von **[Enabled (Aktiviert)]** auf **[Mixed (Gemischt)]** oder **[Disabled (Deaktiviert)]** ändern, kann der Desktop immer noch nicht gestartet werden. Um einen Desktop nach dem Ändern des Sicherheitsmodus für Nachrichten von **[Enabled (Aktiviert)]** in **[Mixed (Gemischt)]** oder **[Disabled (Deaktiviert)]** zu starten, müssen Sie den Desktop neu starten.

Wenn Sie vorhaben, eine aktive View-Umgebung von **[Disabled (Deaktiviert)]** in **[Enabled (Aktiviert)]** oder von **[Enabled (Aktiviert)]** in **[Disabled (Deaktiviert)]** zu ändern, wechseln Sie für einen kurzen Zeitraum vor der endgültigen Änderung in den Modus **[Mixed (Gemischt)]** . Wenn Ihr aktueller Modus beispielsweise **[Disabled (Deaktiviert)]** lautet, wechseln Sie für einen Tag in den Modus **[Mixed (Gemischt)]** und danach in **[Enabled (Aktiviert)]** . Im Modus **[Mixed (Gemischt)]** werden Signaturen an die Nachrichten angehängt, aber nicht überprüft, wodurch der Wechsel des Nachrichtenmodus in der gesamten Umgebung übernommen werden kann.

Konfigurieren einer sicheren Tunnelverbindung und eines PCoIP Secure Gateways

Wenn Benutzer sich mit einem View-Desktop verbinden und der sichere Tunnel aktiviert ist, baut View Client eine zweite HTTPS-Verbindung mit dem View Connection Server- oder Sicherheitsserverhost auf.

Wenn Benutzer sich über das PCoIP-Anzeigeprotokoll mit einem View-Desktop verbinden und das PCoIP Secure Gateway aktiviert ist, baut View Client eine weitere sichere Verbindung mit dem View Connection Server- oder Sicherheitsserverhost auf.

Wenn weder der sichere Tunnel noch das PCoIP Secure Gateway aktiviert sind, wird die Desktop-Sitzung direkt zwischen dem Clientsystem und der virtuellen View-Desktop-Maschine hergestellt, und der View Connection Server- oder Sicherheitsserverhost werden umgangen. Dieser Verbindungstyp wird als direkte Verbindung bezeichnet.

Wichtig Eine typische Netzwerkkonfiguration, die sichere Verbindungen für externe Clients bereitstellt, umfasst einen Sicherheitsserver. Wenn Sie View Administrator zum Aktivieren oder Deaktivieren des sicheren Tunnels und des PCoIP Secure Gateways auf einem Sicherheitsserver verwenden möchten, müssen Sie die View Connection Server-Instanz bearbeiten, die mit dem Sicherheitsserver kombiniert ist.

In einer Netzwerkkonfiguration, bei der externe Clients sich direkt mit einem View Connection Server-Host verbinden, aktivieren oder deaktivieren Sie den sicheren Tunnel und das PCoIP Secure Gateway, indem Sie die entsprechende View Connection Server-Instanz in View Administrator bearbeiten.

Voraussetzungen

- Wenn Sie beabsichtigen, das PCoIP Secure Gateway zu aktivieren, stellen Sie sicher, dass die View Connection Server-Instanz und der kombinierte Sicherheitsserver in der Version View 4.6 oder höher vorliegen.
- Wenn Sie einen Sicherheitsserver mit einer View Connection Server-Instanz kombinieren, auf der Sie das PCoIP Secure Gateway bereits aktiviert haben, stellen Sie sicher, dass der Sicherheitsserver in der Version View 4.6 oder höher vorliegt.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie unter **[View Connection Servers (View Connection Server)]** eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Konfigurieren Sie die Verwendung des sicheren Tunnels.

Option	Beschreibung
Deaktivieren des sicheren Tunnels	Deaktivieren Sie **[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]** .
Aktivieren des sicheren Tunnels	Aktivieren Sie **[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]** .

Der sichere Tunnel ist standardmäßig aktiviert.

4 Konfigurieren Sie die Verwendung des PCoIP Secure Gateways.

Option	Beschreibung
Aktivieren des PCoIP Secure Gateways	Wählen Sie **[Use PCoIP Secure Gateway for PCoIP connections to desktop (PCoIP Secure Gateway für PCoIP-Verbindungen mit dem Desktop verwenden]**
Deaktivieren des PCoIP Secure Gateways	Heben Sie die Auswahl von **[Use PCoIP Secure Gateway for PCoIP connections to desktop (PCoIP Secure Gateway für PCoIP-Verbindungen mit dem Desktop verwenden]** auf.

Das PCoIP Secure Gateway ist standardmäßig deaktiviert.

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Festlegen eines SSO-Zeitüberschreitungslimits für View-Benutzer

Bei der Benutzeranmeldung an View Connection Server über View Client ist standardmäßig die einmalige Anmeldung (Single Sign-On, SSO) aktiviert. Der Benutzer muss sich nicht erneut anmelden, um eine Verbindung mit dem View-Desktop herzustellen. Wenn ein Benutzer den Desktop während einer Desktop-Sitzung verlässt und der Desktop nach einer gewissen Zeit in den Leerlauf wechselt, kann der Benutzer anschließend erneut zum Desktop wechseln, ohne sich erneut anmelden zu müssen. Um die Wahrscheinlichkeit eines Starts durch einen anderen Benutzer über die Desktop-Sitzung zu minimieren, können Sie ein Zeitlimit festlegen, nach Ablauf dessen die SSO-Anmeldedaten des Benutzers nicht länger gültig sind.

Sie können das SSO-Zeitüberschreitungslimit konfigurieren, indem Sie einen Wert in View LDAP festlegen. Wenn Sie View LDAP auf einer View Connection Server-Instanz ändern, werden diese Änderungen auf alle replizierten View Connection Server-Instanzen übertragen.

Das Zeitüberschreitungslimit wird in Minuten festgelegt. Der Zeitzähler wird aktiviert, sobald sich der Benutzer an View Connection Server anmeldet. Wenn Sie den Wert beispielsweise auf 10 Minuten festlegen, werden die SSO-Anmeldedaten des Benutzers 10 Minuten nach der Anmeldung an View Connection Server ungültig.

HINWEIS Auf View-Desktops im lokalen Modus verursacht ein Auscheckvorgang, der länger als das festgelegte SSO-Zeitüberschreitungslimit dauert, einen Ablauf der SSO-Anmeldedaten. Angenommen, Sie legen das SSO-Zeitüberschreitungslimit auf 10 Minuten fest. Ein Benutzer meldet sich an View Connection Server an und checkt einen Desktop aus. Wenn der Auscheckvorgang länger als 20 Minuten dauert, muss sich der Benutzer zur Verbindungsherstellung mit dem lokalen Desktop erneut anmelden – selbst wenn der Benutzer noch keine Zeit in einer Desktop-Sitzung verbracht hat.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion.

Vorgehensweise

1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host.

2 Wählen Sie oder stellen Sie eine Verbindung mit **[DC=vdi, DC=vmware, DC=int]** her.

3 Legen Sie für das Objekt **[CN=Common, OU=Global, OU=Properties]** das Attribut **[pae-SSOCredentialCacheTimeout]** auf ein neues SSO-Zeitüberschreitungslimit (in Minuten) fest.

   Der Standardwert lautet 15. Ein Wert von -1 bedeutet, dass kein SSO-Zeitüberschreitungslimit festgelegt ist. Mit dem Wert 0 wird die einmalige Anmeldung (SSO) deaktiviert.

Auf Remote-Desktops tritt das neue SSO-Zeitüberschreitungslimit sofort in Kraft. Der View Connection Server-Dienst oder der Clientcomputer müssen nicht neu gestartet werden.

Auf Desktops im lokalen Modus wird das neue SSO-Zeitüberschreitungslimit wirksam, sobald ein Clientcomputer, der den lokalen Desktop hostet, das nächste Mal eine Taktsignalmeldung an View Connection Server sendet.

Deaktivieren oder Aktivieren von View Connection Server

Sie können eine View Connection Server-Instanz deaktivieren, um die Anmeldung von Benutzern an ihren View-Desktops zu verhindern. Wenn Sie eine Instanz deaktivieren, können Sie sie wieder aktivieren.

Benutzer, die derzeit an ihren View-Desktops angemeldet sind, sind von der Deaktivierung einer View Connection Server-Instanz nicht betroffen.

Mit Ihrer View Manager-Bereitstellung wird bestimmt, inwiefern Benutzer durch das Deaktivieren einer Instanz betroffen sind.

- Wenn es sich um eine einzelne, eigenständige View Connection Server-Instanz handelt, können sich Benutzer an ihren Desktops nicht anmelden. Sie können keine Verbindung mit View Connection Server herstellen.
- Wenn es sich um eine replizierte View Connection Server-Instanz handelt, wird mit Ihrer Netzwerktopologie bestimmt, ob Benutzer zu einer anderen replizierten Instanz weitergeleitet werden. Wenn Benutzer auf eine andere Instanz zugreifen können, können sie sich an ihren Desktops anmelden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie im Fensterbereich **[View Connection Servers (View Connection Server)]** die View Connection Server-Instanz aus.

3 Klicken Sie auf **[Disable (Deaktivieren)]** .

Sie können die Instanz erneut aktivieren, indem Sie auf **[Enable (Aktivieren)]** klicken.

Bearbeiten der externen URLs

Sie können zum Bearbeiten von externen URLs für View Connection Server-Instanzen und Sicherheitsservern View Administrator verwenden.

Ein View Connection Server- oder Sicherheitsserverhost können standardmäßig nur über Tunnelclients kontaktiert werden, die sich im selben Netzwerk befinden. Tunnelclients, die außerhalb Ihres Netzwerks ausgeführt werden, müssen eine durch den Client auflösbare URL zur Verbindungsherstellung mit einem View Connection Server- oder Sicherheitsserver-Host verwenden.

Wenn Benutzer mit dem PCoIP-Anzeigeprotokoll eine Verbindung mit View-Desktops herstellen, kann View Client eine weitere Verbindung mit dem sicheren PCoIP-Gateway auf dem View Connection Server- oder Sicherheitsserverhost aufbauen. Zur Verwendung des PCoIP Secure Gateway muss ein Clientsystem auf eine IP-Adresse zugreifen können, die dem Client eine Verbindungsherstellung mit dem View Connection Server- oder Sicherheitsserverhost ermöglicht. Sie geben diese IP-Adresse in der externen PCoIP-URL an.

Sowohl bei der externen URL des sicheren Tunnels als auch bei der externen URL des PCoIP muss es sich um die Adressen handeln, die die Clientsysteme zum Erreichen des Hosts verwenden. Geben Sie beispielsweise bei der Konfiguration eines View Connection Server-Hosts weder die externe URL des sicheren Tunnels für diesen Host noch die externe PCoIP-URL für einen kombinierten Sicherheitsserver an.

HINWEIS Für einen Sicherheitsserver, der nicht auf View Connection Server 4.5 oder höher aktualisiert wurde, können Sie die externen URLs nicht bearbeiten.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)]** > **[Server]** .

Option	Aufgabe
View Connection Server-Instanz	Wählen Sie die View Connection Server-Instanz im Bereich **[View Connection Servers (View Connection Server)]** aus und klicken Sie auf **[Edit (Bearbeiten)]** .
Sicherheitsserver	Wählen Sie den Sicherheitsserver im Bereich **[Security Servers (Sicherheitsserver)]** aus und klicken Sie auf **[Edit (Bearbeiten)]** .

2 Geben Sie im Textfeld **[External URL (Externe URL)]** die externe URL des sicheren Tunnels ein.

Die URL muss das Protokoll, den durch den Client auflösbaren Hostnamen oder die IP-Adresse sowie die Portnummer enthalten.

Beispiel: https://view.example.com:443

3 Geben Sie im Textfeld **[PCoIP External URL (PCoIP – Externe URL)]** die externe URL des sicheren PCoIP-Gateways ein.

Geben Sie die externe PCoIP-URL als IP-Adresse mit der Portnummer 4172 ein. Schließen Sie keinen Protokollnamen ein.

Beispiel: `100.200.300.400:4172`

Die URL muss die IP-Adresse und Portnummer enthalten, die ein Clientsystem zur Verbindungsherstellung mit dieser Sicherheitsserver- oder View Connection Server-Instanz benötigt. Sie können nur dann eine Eingabe in diesem Textfeld vornehmen, wenn auf der Sicherheitsserver- oder View Connection Server-Instanz ein PCoIP Secure Gateway installiert ist.

4 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Die externen URLs werden sofort aktualisiert. Sie müssen den View Connection Server- oder den Sicherheitsserverdienst nicht neu starten, damit die Änderungen wirksam werden.

View LDAP-Verzeichnis

View LDAP ist das Daten-Repository für alle View Manager-Konfigurationsinformationen. View LDAP ist ein eingebettetes LDAP-Verzeichnis (Lightweight Directory Access Protocol), das mit der View Connection Server-Installation bereitgestellt wird.

View LDAP umfasst die standardmäßigen LDAP-Verzeichniskomponenten, die in View Manager verwendet werden.

- View Manager-Schemadefinitionen
- DIT-Definitionen (Directory Information Tree)
- Zugriffssteuerungslisten (Access Control Lists, ACLs)

View LDAP enthält Verzeichniseinträge, die View Manager-Objekte repräsentieren.

- View-Desktop-Einträge, die jeden Desktop darstellen, auf den zugegriffen werden kann. Jeder Eintrag enthält Referenzen zu den FSP-Einträgen (Foreign Security Principal) der Windows-Benutzer und -gruppen im Active Directory, die den Desktop nutzen dürfen.
- View-Desktop-Pool-Einträge, die mehrere virtuelle Desktops, die gemeinsam verwaltet werden, repräsentieren.
- Einträge für virtuelle Maschinen, die die virtuelle vCenter Server-Maschine für jeden Desktop repräsentieren.
- View Manager-Komponenteneinträge, die Konfigurationseinstellungen speichern

View LDAP umfasst außerdem einen Satz von Plug-In-DLLs für View Manager, die Automatisierungs- und Benachrichtigungsdienste für andere View Manager-Komponenten bereitstellen.

HINWEIS Sicherheitsserverinstanzen haben kein View LDAP-Verzeichnis.

Konfigurieren von View Connection Server-Einstellungen

Sie können View Administrator zum Bearbeiten von Konfigurationseinstellungen für View Connection Server-Instanzen verwenden.

Konfigurieren der rollenbasierten Verwaltungsdelegierung 2

Eine wichtige Verwaltungsaufgabe in einer View-Umgebung besteht darin festzustellen, wer View Administrator verwenden kann und zur Ausführung welcher Aufgaben diese Benutzer autorisiert sind. Bei der rollenbasierten Verwaltungsdelegierung können Sie Administratorberechtigungen gezielt zuweisen, indem Sie bestimmten Active Directory-Benutzern und -Gruppen Administratorrollen zuweisen.

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlegendes zu Rollen und Berechtigungen“, auf Seite 27
- „Verwenden von Ordnern für die Verwaltungsdelegierung“, auf Seite 28
- „Grundlegendes zu Berechtigungen“, auf Seite 29
- „Verwalten von Administratoren“, auf Seite 30
- „Verwalten und Überprüfen von Berechtigungen“, auf Seite 32
- „Verwalten und Überprüfen von Ordnern“, auf Seite 34
- „Verwalten von benutzerdefinierten Rollen“, auf Seite 36
- „Vordefinierte Rollen und Berechtigungen“, auf Seite 38
- „Erforderliche Berechtigungen für häufige Aufgaben“, auf Seite 42
- „Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen“, auf Seite 45

Grundlegendes zu Rollen und Berechtigungen

Die Möglichkeit, Aufgaben in View Administrator auszuführen, wird durch ein Zugriffssteuerungssystem bestimmt, das Administratorrollen und -berechtigungen umfasst. Dieses System ist mit dem vCenter Server-Zugriffssteuerungssystem vergleichbar.

Eine Administratorrolle ist eine Sammlung aus Berechtigungen. Berechtigungen befähigen zur Durchführung bestimmter Aktionen, beispielsweise zum Gewähren von Benutzerberechtigungen für einen Desktop-Pool. Berechtigungen steuern außerdem, welche Objekte ein Administrator in View Administrator anzeigen kann. Wenn ein Administrator beispielsweise keine Berechtigungen zum Anzeigen oder Ändern globaler Richtlinien besitzt, ist die Einstellung **[Global Policies (Globale Richtlinien)]** nicht im Navigationsbereich sichtbar, wenn sich der Administrator an View Administrator anmeldet.

Administratorberechtigungen sind entweder global oder objektspezifisch. Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Bestandslistenobjekten.

Administratorrollen kombinieren typischerweise alle Berechtigungen, die zum Durchführen einer Verwaltungsaufgabe höherer Ebene erforderlich sind. View Administrator umfasst vordefinierte Rollen, welche die zur Ausführung häufiger Verwaltungsaufgaben erforderlichen Berechtigungen enthalten. Sie können diese vordefinierten Rollen Administratorbenutzern und -gruppen zuweisen oder eigene Rollen erstellen, indem Sie ausgewählte Berechtigungen miteinander kombinieren. Die vordefinierten Rollen können nicht geändert werden.

Sie erstellen Administratoren, indem Sie Benutzer und Gruppen aus Ihren Active Directory-Benutzern und -Gruppen auswählen und diesen Administratorrollen zuweisen. Administratoren erhalten Berechtigungen über ihre Rollenzuweisungen. Berechtigungen können Administratoren nicht direkt zugewiesen werden. Ein Administrator mit mehreren Rollenzuweisungen erhält die Summe aller Berechtigungen in diesen Rollen.

Verwenden von Ordnern für die Verwaltungsdelegierung

Standardmäßig werden Desktop-Pools im Stammordner erstellt, der in View Administrator als / oder Root(/) angezeigt wird. Sie können unterhalb des Stammordners Ordner erstellen, um Ihre Desktop-Pools zu unterteilen und die Verwaltung bestimmter Desktop-Pools an unterschiedliche Administratoren zu delegieren.

Ein Desktop erbt die Ordner von seinem Pool. Eine verbundene persistente Festplatte erbt den Ordner vom zugehörigen Desktop. Sie können über maximal 100 Ordner verfügen (einschließlich Stammordner).

Sie konfigurieren den Administratorzugriff auf die Ressourcen in einem Ordner, indem Sie einem Administrator für diesen Ordner eine Rolle zuweisen. Administratoren können ausschließlich auf Ressourcen in Ordnern zugreifen, für die ihnen Rollen zugewiesen wurden. Die Rolle, die einem Administrator für einen Ordner zugewiesen wurde, bestimmt die Zugriffsebene des Administrators für die Ressourcen in diesem Ordner.

Da Rollen vom Stammordner geerbt werden, verfügt ein Administrator mit einer Rolle für den Stammordner für sämtliche Ordner über diese Rolle. Administratoren mit der Administratorenrolle für den Stammordner sind übergeordnete Administratoren, da sie über Vollzugriff auf alle Bestandslistenobjekte innerhalb des Systems verfügen.

Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf einen Ordner angewendet werden zu können. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Ordner angewendet werden.

Sie können mithilfe von View Administrator Ordner erstellen und vorhandene Pools in Ordner verschieben. Sie können auch einen Ordner auswählen, wenn Sie einen Desktop-Pool erstellen. Wenn Sie während der Pool-Erstellung keinen Ordner auswählen, wird der Pool standardmäßig im Stammordner erstellt.

- Verschiedene Administratoren für verschiedene Ordner auf Seite 28

  Sie können unterschiedliche Administratoren zur Verwaltung verschiedener Ordner in Ihrer Konfiguration erstellen.

- Verschiedene Administratoren für denselben Ordner auf Seite 29

  Sie können unterschiedliche Administratoren zur Verwaltung desselben Ordners erstellen.

Verschiedene Administratoren für verschiedene Ordner

Sie können unterschiedliche Administratoren zur Verwaltung verschiedener Ordner in Ihrer Konfiguration erstellen.

Wenn sich Ihre Unternehmens-Desktop-Pools beispielsweise in einem anderen Ordner befinden als die Desktop-Pools für die Softwareentwickler, können Sie unterschiedliche Administratoren zum Verwalten der Ordner in jedem dieser Ordner erstellen.

Tabelle 2-1 zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 2-1. Verschiedene Administratoren für verschiedene Ordner

Administrator	Rolle	Ordner
view-domain.com\Admin1	Inventory Administrators (Bestandslistenadministratoren)	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators (Bestandslistenadministratoren)	/DeveloperDesktops

In diesem Beispiel wurde dem Administrator „Admin1“ die Rolle **[Inventory Administrators (Bestandslistenadministratoren)]** für den Ordner `CorporateDesktops` zugewiesen. Der Administrator „Admin2“ verfügt für den Ordner `DeveloperDesktops` über die Rolle **[Inventory Administrators (Bestandslistenadministratoren)]** .

Verschiedene Administratoren für denselben Ordner

Sie können unterschiedliche Administratoren zur Verwaltung desselben Ordners erstellen.

Wenn sich Ihre Unternehmens-Desktop-Pools beispielsweise in einem Ordner befinden, können Sie einen Administrator erstellen, der diese Pools anzeigen und ändern kann, sowie einen weiteren Administrator, der die Pools nur anzeigen kann.

Tabelle 2-2 zeigt ein Beispiel für diese Art der Konfiguration.

Tabelle 2-2. Verschiedene Administratoren für denselben Ordner

Administrator	Rolle	Ordner
view-domain.com\Admin1	Inventory Administrators (Bestandslistenadministratoren)	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators (Read Only) (Bestandslistenadministratoren (Nur Lesen))	/CorporateDesktops

In diesem Beispiel wurde dem Administrator „Admin1“ die Rolle **[Inventory Administrators (Bestandlistenadministratoren)]** für den Ordner `CorporateDesktops` zugewiesen. Der Administrator „Admin2“ verfügt für denselben Ordner über die Rolle **[Inventory Administrators (Read only) (Bestandslistenadministratoren (Nur Lesen))]** .

Grundlegendes zu Berechtigungen

View Administrator stellt die Kombination einer Rolle, eines Administratorbenutzers oder einer Administratorgruppe sowie eines Ordners als Berechtigung dar. Die Rolle definiert die Aktionen, die ausgeführt werden können, der Benutzer oder die Gruppe gibt an, wer die Aktion ausführen kann, und der Ordner enthält die Objekte, die Ziel der Aktion sind.

Berechtigungen werden in View Administrator unterschiedlich angezeigt, abhängig davon, ob Sie einen Administratorbenutzer oder eine Administratorgruppe, einen Ordner oder eine Rolle auswählen.

Tabelle 2-3 zeigt, wie Berechtigungen in View Administrator angezeigt werden, wenn Sie einen Administratorbenutzer oder eine Administratorgruppe auswählen. Der Administratorbenutzer heißt „Admin 1“ und verfügt über zwei Berechtigungen.

Tabelle 2-3. Berechtigungen auf der Registerkarte „Administrators and Groups (Administratoren und Gruppen)“ für Admin 1

Rolle	Ordner
Inventory Administrators (Bestandslistenadministratoren)	MarketingDesktops
Administrators (Read Only) (Administratoren (Nur Lesen))	/

Die erste Berechtigung zeigt, dass Admin 1 über die Rolle **[Inventory Administrators (Bestandslistenadministratoren)]** für den Ordner `MarketingDesktops` verfügt. Die zweite Berechtigung zeigt, dass Admin 1 über die Rolle **[Administrators (Read Only) (Administratoren (Nur Lesen))]** für den Stammordner verfügt.

Tabelle 2-4 zeigt, wie dieselben Berechtigungen in View Administrator angezeigt werden, wenn Sie den Ordner `MarketingDesktops` auswählen.

Tabelle 2-4. Berechtigungen auf der Registerkarte „Folders (Ordner)“ für „MarketingDesktops“

Admin	Rolle	Vererbt
view-domain.com\Admin1	Inventory Administrators (Bestandslistenadministratoren)	
view-domain.com\Admin1	Administrators (Read Only) (Administratoren (Nur Lesen))	Ja.

Die erste Berechtigung ist dieselbe wie die erste Berechtigung in Tabelle 2-3. Die zweite Berechtigung wird von der zweiten Berechtigung geerbt, wie gezeigt in Tabelle 2-3. Da Ordner die Berechtigungen vom Stammordner erben, verfügt Admin 1 über die Rolle **[Administrators (Read Only) (Administratoren (Nur Lesen))]** für den Ordner `MarketingDesktops`. Wenn eine Berechtigung vererbt wurde, erscheint in der Spalte **[Inherited (Vererbt)]** der Wert **[Yes (Ja)]** .

Tabelle 2-5 zeigt, wie die erste Berechtigung in Tabelle 2-3 in View Administrator angezeigt wird, wenn Sie die Rolle **[Inventory Administrators (Bestandslistenadministratoren)]** auswählen.

Tabelle 2-5. Berechtigungen auf der Registerkarte „Role (Rolle)“ für Bestandslistenadministratoren

Administrator	Ordner
view-domain.com\Admin1	`/MarketingDesktops`

Verwalten von Administratoren

Benutzer mit der Administratorrolle können View Administrator zum Hinzufügen und Entfernen von Administratorbenutzern und -gruppen verwenden.

Die Administratorrolle ist die einflussreichste Rolle in View Administrator. Anfänglich wird Mitgliedern der lokalen Administratorengruppe (BUILTIN\Administrators) auf Ihrem View Connection Server-Host die Administratorrolle in View Administrator zugewiesen.

Hinweis Die Gruppe **[Domain Admins (Domänen-Admins)]** ist standardmäßig Mitglied der lokalen Administratorengruppe. Wenn die Domänenadministratoren nicht über Vollzugriff auf Bestandslistenobjekte und View-Konfigurationseinstellungen verfügen sollen, muss die Gruppe **[Domain Admins (Domänen-Admins)]** aus der lokalen Administratorengruppe entfernt werden.

- Erstellen eines Administrators auf Seite 31

  Um einen Administrator zu erstellen, wählen Sie in View Administrator einen Benutzer oder eine Gruppe aus den Active Directory-Benutzern und -Gruppen aus und weisen dem Benutzer bzw. der Gruppe eine Administratorrolle zu.

- Entfernen eines Administrators auf Seite 32

  Sie können einen Administratorbenutzer oder eine Administratorgruppe entfernen. Der letzte übergeordnete Administrator innerhalb des Systems kann nicht entfernt werden. Bei einem übergeordneten Administrator handelt es sich um einen Administrator mit der Administratorenrolle für den Stammordner.

Erstellen eines Administrators

Um einen Administrator zu erstellen, wählen Sie in View Administrator einen Benutzer oder eine Gruppe aus den Active Directory-Benutzern und -Gruppen aus und weisen dem Benutzer bzw. der Gruppe eine Administratorrolle zu.

Voraussetzungen

- Machen Sie sich mit den vordefinierten Administratorrollen vertraut. Siehe „Vordefinierte Rollen und Berechtigungen“, auf Seite 38.
- Machen Sie sich mit den empfohlenen Vorgehensweisen für das Erstellen von Administratorbenutzern und -gruppen vertraut. Siehe „Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen“, auf Seite 45.
- Um dem Administrator eine benutzerdefinierte Rolle zuzuweisen, erstellen Sie die benutzerdefinierte Rolle. Siehe „Hinzufügen einer benutzerdefinierten Rolle“, auf Seite 36.
- Zum Erstellen eines Administrators, der bestimmte Desktop-Pools verwalten darf, erstellen Sie einen Ordner und verschieben Sie die Desktop-Pools in diesen Ordner. Siehe „Verwalten und Überprüfen von Ordnern“, auf Seite 34.

Vorgehensweise

1. Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .
2. Klicken Sie auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** auf **[Add User or Group (Benutzer oder Gruppe hinzufügen)]** .
3. Klicken Sie auf **[Add (Hinzufügen)]** , wählen Sie mindestens ein Suchkriterium und klicken Sie auf **[Find (Suchen)]** , um basierend auf den angegebenen Suchkriterien nach Active Directory-Benutzern oder -Gruppen zu filtern.
4. Wählen Sie den Active Directory-Benutzer bzw. die Active Directory-Gruppe, den/die Sie als Administratorbenutzer oder -gruppe konfigurieren möchten, klicken Sie auf **[OK]** und anschließend auf **[Next (Weiter)]** .

   Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen.
5. Wählen Sie eine Rolle, die Sie dem Administratorbenutzer oder der Administratorgruppe zuweisen möchten.

   Die Spalte **[Apply to Folder (Auf Ordner anwenden)]** gibt an, ob eine Rolle auf Ordner angewendet werden kann. Nur Rollen, die objektspezifische Berechtigungen enthalten, können auf Ordner angewendet werden. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Ordner angewendet werden.

Option	Aktion
Die ausgewählte Rolle gilt für Ordner	Wählen Sie einen oder mehrere Ordner aus und klicken Sie auf **[Next (Weiter)]** .
Die Berechtigung soll für alle Ordner gelten	Wählen Sie den Stammordner aus und klicken Sie auf **[Next (Weiter)]** .

6. Klicken Sie auf **[Finish (Fertig stellen)]** , um den Administratorbenutzer oder die Administratorgruppe zu erstellen.

Der neue Administratorbenutzer bzw. die Administratorgruppe wird im linken Fensterbereich angezeigt. Die ausgewählte Rolle und der ausgewählte Ordner werden im rechten Fensterbereich auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** angezeigt.

Entfernen eines Administrators

Sie können einen Administratorbenutzer oder eine Administratorgruppe entfernen. Der letzte übergeordnete Administrator innerhalb des Systems kann nicht entfernt werden. Bei einem übergeordneten Administrator handelt es sich um einen Administrator mit der Administratorenrolle für den Stammordner.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Wählen Sie auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** den Administratorbenutzer oder die Administratorgruppe, klicken Sie auf **[Remove User or Group (Benutzer oder Gruppe entfernen)]** und anschließend auf **[OK]** .

Der Administratorbenutzer oder die Administratorgruppe wird nicht länger auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** angezeigt.

Verwalten und Überprüfen von Berechtigungen

Sie können mithilfe von View Administrator Berechtigungen für spezifische Administratorbenutzer und -gruppen bzw. bestimmte Rollen und Ordner hinzufügen, löschen und überprüfen.

- Hinzufügen einer Berechtigung auf Seite 32

  Sie können eine Berechtigung hinzufügen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfasst.

- Löschen einer Berechtigung auf Seite 33

  Sie können eine Berechtigung löschen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfasst.

- Überprüfen von Berechtigungen auf Seite 34

  Sie können die Berechtigungen überprüfen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfassen.

Hinzufügen einer Berechtigung

Sie können eine Berechtigung hinzufügen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfasst.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Erstellen Sie die Berechtigung.

Option	Aktion
Erstellen einer Berechtigung, die einen bestimmten Administratorbenutzer oder eine bestimmte Administratorgruppe umfasst	a Wählen Sie auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** den Administrator oder die Administratorgruppe und klicken Sie auf **[Add Permission (Berechtigung hinzufügen)]** . b Wählen Sie eine Rolle. c Wenn die Rolle nicht auf Ordner angewendet wird, klicken Sie auf **[Finish (Fertig stellen)]** . d Wenn die Rolle auf Ordner angewendet wird, klicken Sie auf **[Next (Weiter)]** , wählen Sie einen oder mehrere Ordner aus und klicken Sie auf **[Finish (Fertig stellen)]** . Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf einen Ordner angewendet werden zu können.
Erstellen einer Berechtigung, die eine bestimmte Rolle umfasst	a Wählen Sie auf der Registerkarte **[Roles (Rollen)]** die gewünschte Rolle, klicken Sie auf **[Permissions (Berechtigungen)]** und anschließend auf **[Add Permission (Berechtigung hinzufügen)]** . b Klicken Sie auf **[Add (Hinzufügen)]** , wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **[Find (Suchen)]** , um basierend auf den angegebenen Suchkriterien nach Administratorbenutzern oder -gruppen zu suchen. c Wählen Sie einen Administratorbenutzer oder eine Administratorgruppe, den bzw. die Sie in die Berechtigung einschließen möchten, und klicken Sie auf **[OK]** . Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen. d Wenn die Rolle nicht auf Ordner angewendet wird, klicken Sie auf **[Finish (Fertig stellen)]** . e Wenn die Rolle auf Ordner angewendet wird, klicken Sie auf **[Next (Weiter)]** , wählen Sie einen oder mehrere Ordner aus und klicken Sie auf **[Finish (Fertig stellen)]** . Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf einen Ordner angewendet werden zu können.
Erstellen einer Berechtigung, die einen bestimmten Ordner umfasst	a Wählen Sie auf der Registerkarte **[Folders (Ordner)]** den gewünschten Ordner und klicken Sie auf **[Add Permission (Berechtigung hinzufügen)]** . b Klicken Sie auf **[Add (Hinzufügen)]** , wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **[Find (Suchen)]** , um basierend auf den angegebenen Suchkriterien nach Administratorbenutzern oder -gruppen zu suchen. c Wählen Sie einen Administratorbenutzer oder eine Administratorgruppe, den bzw. die Sie in die Berechtigung einschließen möchten, und klicken Sie auf **[OK]** . Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen. d Klicken Sie auf **[Next (Weiter)]** , wählen Sie eine Rolle und klicken Sie auf **[Finish (Fertig stellen)]** . Eine Rolle muss mindestens eine objektspezifische Berechtigung enthalten, um auf einen Ordner angewendet werden zu können.

Löschen einer Berechtigung

Sie können eine Berechtigung löschen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfasst.

Wenn Sie die letzte Berechtigung für einen Administratorbenutzer oder eine Administratorgruppe entfernen, wird der jeweilige Administratorbenutzer bzw. die Administratorgruppe ebenfalls gelöscht. Da mindestens ein Administrator über die Administratorrolle für den Stammordner verfügen muss, können Sie keine Berechtigung löschen, die zum Entfernen des Administrators führen würde. Eine vererbte Berechtigung kann nicht gelöscht werden.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Wählen Sie die Berechtigung aus, die gelöscht werden soll.

Option	Aktion
Löschen einer Berechtigung, die für einen bestimmten Administrator oder eine bestimmte Gruppe gilt	Wählen Sie den Administrator oder die Gruppe auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** aus.
Löschen einer Berechtigung, die für eine bestimmte Rolle gilt	Wählen Sie die Rolle auf der Registerkarte **[Roles (Rollen)]** aus.
Löschen einer Berechtigung, die für einen bestimmten Ordner gilt	Wählen Sie den Ordner auf der Registerkarte **[Folders (Ordner)]** aus.

3 Wählen Sie die Berechtigung und klicken Sie auf **[Delete Permission (Berechtigung löschen)]** .

Überprüfen von Berechtigungen

Sie können die Berechtigungen überprüfen, die einen bestimmten Administratorbenutzer oder eine Administratorgruppe, eine bestimmte Rolle oder einen bestimmten Ordner umfassen.

Vorgehensweise

1 Wählen Sie **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Überprüfen Sie die Berechtigungen.

Option	Aktion
Überprüfen der Berechtigungen, die einen bestimmten Administrator oder eine bestimmte Gruppe umfassen	Wählen Sie den Administrator oder die Gruppe auf der Registerkarte **[Administrators and Groups (Administratoren und Gruppen)]** aus.
Überprüfen der Berechtigungen, die eine bestimmte Rolle umfassen	Wählen Sie die Rolle auf der Registerkarte **[Roles (Rollen)]** aus und klicken Sie auf **[Permissions (Berechtigungen)]** .
Überprüfen der Berechtigungen, die einen bestimmten Ordner umfassen	Wählen Sie den Ordner auf der Registerkarte **[Folders (Ordner)]** aus.

Verwalten und Überprüfen von Ordnern

Sie können mithilfe von View Administrator Ordner hinzufügen und löschen und die Desktop-Pools und Desktops in einem bestimmten Ordner überprüfen.

- Hinzufügen eines Ordners auf Seite 35

  Wenn Sie die Verwaltung bestimmter Desktops oder Pools an unterschiedliche Administratoren delegieren möchten, müssen Sie Ordner zur Unterteilung Ihrer Desktops oder Pools erstellen. Wenn Sie keine Ordner erstellen, befinden sich alle Desktops und Pools im Stammordner.

- Verschieben eines Desktop-Pools in einen anderen Ordner auf Seite 35

  Nachdem Sie einen Ordner zur Unterteilung Ihrer Desktop-Pools erstellt haben, müssen Sie die gewünschten Desktop-Pools manuell in den neuen Ordner verschieben. Wenn Sie sich dazu entscheiden, die Art der Unterteilung Ihrer Desktop-Pools zu ändern, können Sie Desktop-Pools von einem Ordner in einen anderen verschieben.

- Entfernen eines Ordners auf Seite 35

  Wenn ein Ordner keine Bestandslistenobjekte enthält, kann er entfernt werden. Der Stammordner kann nicht entfernt werden.

- Überprüfen des Desktop-Pools in einem Ordner auf Seite 36

  Sie können in View Administrator alle Desktop-Pools in einem bestimmten Ordner anzeigen.

- Überprüfen der Desktops in einem Ordner auf Seite 36

  Sie können in View Administrator alle Desktops in einem bestimmten Ordner anzeigen. Ein Desktop erbt die Ordner von seinem Pool.

Hinzufügen eines Ordners

Wenn Sie die Verwaltung bestimmter Desktops oder Pools an unterschiedliche Administratoren delegieren möchten, müssen Sie Ordner zur Unterteilung Ihrer Desktops oder Pools erstellen. Wenn Sie keine Ordner erstellen, befinden sich alle Desktops und Pools im Stammordner.

Sie können über maximal 100 Ordner verfügen (einschließlich Stammordner).

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie im Dropdown-Menü **[Folder (Ordner)]** auf der Befehlsleiste die Option **[New Folder (Neuer Ordner)]** .

3 Geben Sie einen Namen und eine Beschreibung für den Ordner ein und klicken Sie auf **[OK]** .

  Die Beschreibung ist optional.

Weiter

Verschieben Sie einen oder mehrere Desktop-Pools in den Ordner.

Verschieben eines Desktop-Pools in einen anderen Ordner

Nachdem Sie einen Ordner zur Unterteilung Ihrer Desktop-Pools erstellt haben, müssen Sie die gewünschten Desktop-Pools manuell in den neuen Ordner verschieben. Wenn Sie sich dazu entscheiden, die Art der Unterteilung Ihrer Desktop-Pools zu ändern, können Sie Desktop-Pools von einem Ordner in einen anderen verschieben.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [Pools]** und wählen Sie den Pool aus.

2 Wählen Sie im Dropdown-Menü **[Folder (Ordner)]** die Option **[Change Folder (Ordner ändern)]** .

3 Wählen Sie den Ordner und klicken Sie auf **[OK]** .

View Administrator verschiebt den Pool in den ausgewählten Ordner.

Entfernen eines Ordners

Wenn ein Ordner keine Bestandslistenobjekte enthält, kann er entfernt werden. Der Stammordner kann nicht entfernt werden.

Voraussetzungen

Wenn der Ordner Bestandslistenobjekte enthält, verschieben Sie die Objekte in einen anderen Ordner oder den Stammordner. Siehe „Verschieben eines Desktop-Pools in einen anderen Ordner“, auf Seite 35.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Wählen Sie auf der Registerkarte **[Folders (Ordner)]** den zu löschenden Ordner und klicken Sie auf **[Remove Folder (Ordner entfernen)]** .

3 Klicken Sie auf **[OK]** , um den Ordner zu entfernen.

Überprüfen des Desktop-Pools in einem Ordner

Sie können in View Administrator alle Desktop-Pools in einem bestimmten Ordner anzeigen.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[Pools]** .

Die Seite **[Pools]** zeigt standardmäßig die Pools in allen Ordnern.

2 Wählen Sie über das Dropdown-Menü **[Folder (Ordner)]** den gewünschten Ordner.

Die Seite **[Pools]** zeigt die Pools im ausgewählten Ordner.

Überprüfen der Desktops in einem Ordner

Sie können in View Administrator alle Desktops in einem bestimmten Ordner anzeigen. Ein Desktop erbt die Ordner von seinem Pool.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[Desktops]** .

Die Seite **[Desktops]** zeigt standardmäßig die Desktops in allen Ordnern an.

2 Wählen Sie über das Dropdown-Menü **[Folder (Ordner)]** den gewünschten Ordner.

Die Seite **[Desktops]** zeigt die Desktops im ausgewählten Ordner.

Verwalten von benutzerdefinierten Rollen

Sie können mithilfe von View Administrator benutzerdefinierte Rollen hinzufügen, ändern und löschen.

- Hinzufügen einer benutzerdefinierten Rolle auf Seite 36

  Wenn die vordefinierten Administratorrollen nicht Ihren Anforderungen entsprechen, können Sie ausgewählte Berechtigungen kombinieren, um eigene Rollen in View Administrator zu erstellen.

- Ändern der Berechtigungen in einer benutzerdefinierten Rolle auf Seite 37

  Sie können die Berechtigungen in einer benutzerdefinierten Rolle ändern. Vordefinierte Administratorrollen können nicht geändert werden.

- Entfernen einer benutzerdefinierten Rolle auf Seite 37

  Wenn eine benutzerdefinierte Rolle nicht in einer Berechtigung enthalten ist, können Sie die Rolle entfernen. Vordefinierte Administratorrollen können nicht entfernt werden.

Hinzufügen einer benutzerdefinierten Rolle

Wenn die vordefinierten Administratorrollen nicht Ihren Anforderungen entsprechen, können Sie ausgewählte Berechtigungen kombinieren, um eigene Rollen in View Administrator zu erstellen.

Voraussetzungen

Machen Sie sich mit den Administratorberechtigungen vertraut, die Sie zum Erstellen benutzerdefinierter Rollen verwenden können. Siehe „Vordefinierte Rollen und Berechtigungen“, auf Seite 38.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Klicken Sie auf der Registerkarte **[Roles (Rollen)]** auf **[Add Role (Rolle hinzufügen)]** .

3 Geben Sie einen Namen und eine Beschreibung für die neue Rolle ein, wählen Sie eine oder mehrere Berechtigungen und klicken Sie auf **[OK]** .

Die neue Rolle wird im linken Fensterbereich angezeigt.

Ändern der Berechtigungen in einer benutzerdefinierten Rolle

Sie können die Berechtigungen in einer benutzerdefinierten Rolle ändern. Vordefinierte Administratorrollen können nicht geändert werden.

Voraussetzungen

Machen Sie sich mit den Administratorberechtigungen vertraut, die Sie zum Erstellen benutzerdefinierter Rollen verwenden können. Siehe „Vordefinierte Rollen und Berechtigungen“, auf Seite 38.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Wählen Sie auf der Registerkarte **[Roles (Rollen)]** die gewünschte Rolle.

3 Klicken Sie auf **[Usage (Verwendung)]** , um die Berechtigungen in der Rolle anzuzeigen, und klicken Sie auf **[Edit (Bearbeiten)]** .

4 Wählen Sie Berechtigungen, oder heben Sie die Auswahl von Berechtigungen auf.

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Entfernen einer benutzerdefinierten Rolle

Wenn eine benutzerdefinierte Rolle nicht in einer Berechtigung enthalten ist, können Sie die Rolle entfernen. Vordefinierte Administratorrollen können nicht entfernt werden.

Voraussetzungen

Wenn die Rolle in einer Berechtigung enthalten ist, löschen Sie die Berechtigung. Siehe „Löschen einer Berechtigung“, auf Seite 33.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** .

2 Wählen Sie auf der Registerkarte **[Roles (Rollen)]** die gewünschte Rolle und klicken Sie auf **[Remove Role (Rolle entfernen)]** .

Die Schaltfläche **[Remove Role (Rolle entfernen)]** steht für vordefinierte Rollen oder für benutzerdefinierte Rollen, die in einer Berechtigung enthalten sind, nicht zur Verfügung.

3 Klicken Sie auf **[OK]** , um die Rolle zu entfernen.

Vordefinierte Rollen und Berechtigungen

View Administrator umfasst vordefinierte Rollen, die Sie Ihren Administratorbenutzern und -gruppen zuweisen können. Sie können auch eigene Administratorrollen erstellen, indem Sie ausgewählte Berechtigungen kombinieren.

- Vordefinierte Administratorrollen auf Seite 38

  Die vordefinierten Administratorrollen kombinieren die einzelnen Berechtigungen, die zur Ausführung allgemeiner Verwaltungsaufgaben erforderlich sind. Die vordefinierten Rollen können nicht geändert werden.

- Globale Berechtigungen auf Seite 40

  Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Ordner angewendet werden.

- Objektspezifische Berechtigungen auf Seite 41

  Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Bestandslistenobjekten. Rollen, die objektspezifische Berechtigungen enthalten, können auf Ordner angewendet werden.

- Interne Berechtigungen auf Seite 42

  Einige der vordefinierten Administratorrollen können interne Berechtigungen enthalten. Beim Erstellen benutzerdefinierter Rollen können keine internen Berechtigungen ausgewählt werden.

Vordefinierte Administratorrollen

Die vordefinierten Administratorrollen kombinieren die einzelnen Berechtigungen, die zur Ausführung allgemeiner Verwaltungsaufgaben erforderlich sind. Die vordefinierten Rollen können nicht geändert werden.

Tabelle 2-6 beschreibt die vordefinierten Rollen und gibt an, ob eine Rolle auf einen Ordner angewendet werden kann.

Tabelle 2-6. Vordefinierte Rollen in View Administrator

Rolle	Benutzerfähigkeiten	Gilt für einen Ordner
Administrators (Administratoren)	Durchführen aller Administratoraufgaben wie das Erstellen weiterer Benutzer und Gruppen mit Administratorrechten. Administratoren mit der Administratorenrolle für den Stammordner sind übergeordnete Administratoren, da sie über Vollzugriff auf alle Bestandslistenobjekte innerhalb des Systems verfügen. Da die Administratorenrolle sämtliche Berechtigungen umfasst, sollte sie einer eingeschränkten Anzahl an Benutzern zugewiesen werden. Anfänglich wird Mitgliedern der lokalen Administratorengruppe auf Ihrem View Connection Server-Host diese Rolle für den Stammordner zugewiesen. **WICHTIG** Ein Administrator muss zur Ausführung der folgenden Aufgaben über die Administratorenrolle für den Stammordner verfügen: ■ Hinzufügen und Löschen von Ordnern. ■ Verwalten von ThinApp-Anwendungen und Konfigurationseinstellungen in View Administrator. ■ Anzeigen und Ändern von View Transfer Server-Instanzen sowie des Transfer Server-Repositorys. ■ Verwenden der Befehle `vdmadmin` und `vdmimport`.	Ja.
Administrators (Read Only) (Administratoren (Nur Lesen))	■ Anzeigen von globalen Einstellungen und Bestandslistenobjekten, jedoch keine Berechtigung zum Ändern dieser Elemente und Einstellungen. ■ Anzeigen von ThinApp-Anwendungen und -Einstellungen, View Transfer Server-Instanzen und des Transfer Server-Repositorys, jedoch keine Berechtigung zum Ändern dieser Elemente und Einstellungen. ■ Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme einschließlich `vdmexport`, jedoch mit Ausnahme von `vdmadmin` und `vdmimport`. Wenn Administratoren über diese Rolle für einen Ordner verfügen, können sie die Bestandsobjekte in diesem Ordner nur anzeigen.	Ja.
Agent Registration Administrators (Agent-Registrierungsadministratoren)	Registrieren nicht verwalteter Desktop-Quellen, z.B. physische Systeme, eigenständige virtuelle Maschinen und Terminalserver.	No (Nein)
Global Configuration and Policy Administrators (Globale Konfiguration und Richtlinienadministratoren)	Anzeigen und Ändern von globalen Richtlinien und Konfigurationseinstellungen (mit Ausnahme von Administratorrollen und -berechtigungen), ThinApp-Anwendungen und -Einstellungen, View Transfer Server-Instanzen und des Transfer Server-Repositorys.	No (Nein)
Global Configuration and Policy Administrators (Read only) (Globale Konfiguration und Richtlinienadministratoren (Nur Lesen))	Anzeigen von globalen Richtlinien und Konfigurationseinstellungen (mit Ausnahme von Administratorrollen und -berechtigungen), ThinApp-Anwendungen und -Einstellungen, View Transfer Server-Instanzen und des Transfer Server-Repositorys, jedoch keine Berechtigung zum Ändern dieser Elemente und Einstellungen.	No (Nein)

Tabelle 2-6. Vordefinierte Rollen in View Administrator (Fortsetzung)

Rolle	Benutzerfähigkeiten	Gilt für einen Ordner
Inventory Administrators (Bestandslistenadministratoren)	■ Durchführen aller Desktop-, Sitzungs- und poolbezogenen Vorgänge. ■ Verwalten persistenter Festplatten. ■ Neusynchronisieren, Aktualisieren und Neuverteilen von Linked-Clone-Pools sowie Ändern des standardmäßigen Pool-Images. Wenn Administratoren über diese Rolle für einen Ordner verfügen, können sie diese Vorgänge nur für die Bestandsobjekte in diesem Ordner ausführen.	Ja.
Inventory Administrators (Read Only) (Bestandslistenadministratoren (Nur Lesen))	Anzeigen, aber nicht Ändern von Bestandsobjekten. Wenn Administratoren über diese Rolle für einen Ordner verfügen, können sie die Bestandsobjekte in diesem Ordner nur anzeigen.	Ja.

Globale Berechtigungen

Globale Berechtigungen steuern systemweite Vorgänge, beispielsweise das Anzeigen und Ändern globaler Einstellungen. Rollen, die ausschließlich globale Berechtigungen enthalten, können nicht auf Ordner angewendet werden.

Tabelle 2-7 zeigt die globalen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 2-7. Globale Berechtigungen

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Console Interaction (Konsoleninteraktion)	Anmeldung an und Verwendung von View Administrator.	Administrators (Administratoren) Administrators (Read Only) (Administratoren (Nur Lesen)) Inventory Administrators (Bestandslistenadministratoren) Inventory Administrators (Read Only) (Bestandslistenadministratoren (Nur Lesen)) Global Configuration and Policy Administrators (Globale Konfiguration und Richtlinienadministratoren) Global Configuration and Policy Administrators (Read only) (Globale Konfiguration und Richtlinienadministratoren (Nur Lesen))
Direct Interaction (Direkte Interaktion)	Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von `vdmadmin` und `vdmimport`. Administratoren müssen über die Administratorrolle für den Stammordner verfügen, um die Befehle `vdmadmin` und `vdmimport` verwenden zu können.	Administrators (Administratoren) Administrators (Read Only) (Administratoren (Nur Lesen))
Manage Global Configuration and Policies (Globale Konfiguration und Richtlinien verwalten)	Anzeigen und Ändern globaler Richtlinien und Konfigurationseinstellungen, Administratorrollen und -berechtigungen ausgenommen.	Administrators (Administratoren) Global Configuration and Policy Administrators (Globale Konfiguration und Richtlinienadministratoren)

Tabelle 2-7. Globale Berechtigungen (Fortsetzung)

Berechtigung	Benutzerfähigkeiten	Vordefinierte Rollen
Manage Roles and Permissions (Rollen und Berechtigungen verwalten)	Erstellen, Ändern und Löschen von Administratorrollen und -berechtigungen.	Administrators (Administratoren)
Register Agent (Agent registrieren)	Installieren von View Agent auf nicht verwalteten Desktop-Quellen, z.B. auf physischen Systemen, eigenständigen virtuellen Maschinen und Terminalservern. Während der View Agent-Installation müssen Sie Ihre Administratoranmeldeinformationen angeben, um die nicht verwaltete Desktop-Quelle bei der View Connection Server-Instanz zu registrieren.	Administrators (Administratoren) Agent Registration Administrators (Agent-Registrierungsadministratoren)

Objektspezifische Berechtigungen

Objektspezifische Berechtigungen steuern Vorgänge für bestimmte Arten von Bestandslistenobjekten. Rollen, die objektspezifische Berechtigungen enthalten, können auf Ordner angewendet werden.

Tabelle 2-8 beschreibt die objektspezifischen Berechtigungen. Die vordefinierten Rollen **[Administrators (Administratoren)]** und **[Inventory Administrators (Bestandslistenadministratoren)]** umfassen all diese Berechtigungen.

Tabelle 2-8. Objektspezifische Berechtigungen

Berechtigung	Benutzerfähigkeiten	Objekt
Enable Pool (Pool aktivieren)	Aktivieren und Deaktivieren von Desktop-Pools.	Desktop-Pool
Entitle Pool (Gewähren von Berechtigungen für Pool)	Hinzufügen und Entfernen von Benutzerberechtigungen.	Desktop-Pool
Manage Composer Pool Image (Composer-Pool-Image verwalten)	Neusynchronisieren, Aktualisieren und Neuverteilen von Linked-Clone-Pools sowie Ändern des standardmäßigen Pool-Images.	Desktop-Pool
Manage Desktop (Desktop verwalten)	Durchführen aller Desktop- und sitzungsbezogenen Vorgänge.	Desktop
Manage Local Sessions (Lokale Sitzungen verwalten)	Durchführen von Rollbacks und Initialisieren von Replikationen für lokale Desktops.	Desktop
Manage Persistent Disks (Persistente Festplatten verwalten)	Durchführen aller View Composer-Vorgänge für persistente Festplatten, einschließlich Verknüpfen, Trennen und Importieren von persistenten Festplatten.	Persistente Festplatte
Manage Pool (Pool verwalten)	Hinzufügen, Ändern und Löschen von Desktop-Pools und Hinzufügen und Entfernen von Desktops.	Desktop-Pool
Manage Remote Sessions (Remote-Sitzungen verwalten)	Trennen und Abmelden von Remote-Sitzungen und Senden von Nachrichten an Desktop-Benutzer.	Desktop
Manage Reboot Operation (Neustart verwalten)	Zurücksetzen von Desktops.	Desktop

Interne Berechtigungen

Einige der vordefinierten Administratorrollen können interne Berechtigungen enthalten. Beim Erstellen benutzerdefinierter Rollen können keine internen Berechtigungen ausgewählt werden.

Tabelle 2-9 zeigt die internen Berechtigungen sowie die vordefinierten Rollen, die diese Berechtigungen enthalten.

Tabelle 2-9. Interne Berechtigungen

Berechtigung	Beschreibung	Vordefinierte Rollen
Full (Read only) (Vollständig (Nur Lesen))	Gewährt Lesezugriff auf alle Einstellungen.	Administrators (Read Only) (Administratoren (Nur Lesen))
Manage Inventory (Read only) (Bestandsliste verwalten (Nur Lesen))	Gewährt Lesezugriff auf Bestandslistenobjekte.	Inventory Administrators (Read Only) (Bestandslistenadministratoren (Nur Lesen))
Manage Global Configuration and Policies (Read only) (Globale Konfiguration und Richtlinien verwalten (Nur Lesen))	Gewährt Lesezugriff auf Konfigurationseinstellungen und globale Richtlinien, Administratoren und Rollen ausgenommen.	Global Configuration and Policy Administrators (Read only) (Globale Konfiguration und Richtlinienadministratoren (Nur Lesen))

Erforderliche Berechtigungen für häufige Aufgaben

Viele häufig ausgeführte Verwaltungsaufgaben erfordern einen bestimmten Satz an Berechtigungen. Einige Vorgänge erfordern neben dem Zugriff auf das zu ändernde Objekt Berechtigungen für den Stammordner.

Berechtigungen für die Pool-Verwaltung

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung von Pools in View Administrator verfügen.

Tabelle 2-10 listet gängige Pool-Verwaltungsaufgaben sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Diese Aufgaben werden auf der Seite **[Pools]** in View Administrator ausgeführt.

Tabelle 2-10. Aufgaben und Berechtigungen für die Pool-Verwaltung

Aufgabe	Erforderliche Berechtigungen
Aktivieren oder Deaktivieren eines Pools	**Enable Pool (Pool aktivieren)** für den Pool.
Zuweisen oder Entfernen von Benutzerberechtigungen für einen Pool	**Entitle Pool (Gewähren von Berechtigungen für Pool)** für den Pool.
Hinzufügen eines Pools	**Manage Pool (Pool verwalten)** **Wichtig** Beim Hinzufügen eines Linked-Clone-Pools müssen Sie über die Administratorrolle für den Stammordner verfügen, um das Basis-Image im Transfer Server-Repository zu veröffentlichen.
Ändern oder Löschen eines Pools	**Manage Pool (Pool verwalten)** für den Pool.
Hinzufügen oder Entfernen von Desktops zu bzw. aus einem Pool	**Manage Pool (Pool verwalten)** für den Pool.
Aktualisieren, Neuzusammenstellen, Neuverteilen oder Ändern des standardmäßigen View Composer-Images	**Manage Composer Pool Image (Composer-Pool-Image verwalten)** für den Pool.
Ändern von Ordnern	**[Manage Pool (Pool verwalten)]** für den Quell- und den Zielordner.

Berechtigungen für die Desktop-Verwaltung

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung von Desktops in View Administrator verfügen.

Tabelle 2-11 listet gängige Desktop-Verwaltungsaufgaben sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Diese Aufgaben werden auf der Seite **[Desktops]** in View Administrator ausgeführt.

Tabelle 2-11. Aufgaben und Berechtigungen für die Desktop-Verwaltung

Aufgabe	Erforderliche Berechtigungen
Entfernen einer virtuellen Maschine	**Manage Pool (Pool verwalten)** für den Pool.
Zurücksetzen einer virtuellen Maschine	**Manage Reboot Operation (Neustart verwalten)** für den Desktop.
Abbrechen, Anhalten oder Fortsetzen einer Aufgabe	**Manage Composer Pool Image (Composer-Pool-Image verwalten)**
Zuweisen oder Entfernen von Besitzrechten	**Manage Desktop (Desktop verwalten)** für den Desktop.
Wechseln in den bzw. Beenden des Wartungsmodus	**Manage Desktop (Desktop verwalten)** für den Desktop.
Durchführen von Rollbacks oder Initiieren von Replikationen	**Manage Local Sessions (Lokale Sitzungen verwalten)** für den Desktop.
Trennen oder Abmelden von Remote-Sitzungen	**Manage Remote Sessions (Remote-Sitzungen verwalten)** für den Desktop.

Berechtigungen für die Verwaltung persistenter Festplatten

Administratoren müssen über bestimmte Berechtigungen für die Verwaltung persistenter Festplatten in View Administrator verfügen.

Tabelle 2-12 listet gängige Verwaltungsaufgaben für persistente Festplatten sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Diese Aufgaben werden auf der Seite **[Persistent Disks (Persistente Festplatten)]** in View Administrator ausgeführt.

Tabelle 2-12. Aufgaben und Berechtigungen für die Verwaltung persistenter Festplatten

Aufgabe	Erforderliche Berechtigungen
Trennen einer Festplatte	**Manage Persistent Disks (Persistente Festplatten verwalten)** für die Festplatte und **Manage Pool (Pool verwalten)** für den Pool.
Verknüpfen einer Festplatte	**Manage Persistent Disks (Persistente Festplatten verwalten)** für die Festplatte und **Manage Pool (Pool verwalten)** für den Desktop.
Bearbeiten einer Festplatte	**Manage Persistent Disks (Persistente Festplatten verwalten)** für die Festplatte und **Manage Pool (Pool verwalten)** für den ausgewählten Pool.
Ändern von Ordnern	**Manage Persistent Disks (Persistente Festplatten verwalten)** für den Quell- und den Zielordner.
Neuerstellen eines Desktops	**Manage Persistent Disks (Persistente Festplatten verwalten)** für die Festplatte und **Manage Pool (Pool verwalten)** für den letzten Pool.

Tabelle 2-12. Aufgaben und Berechtigungen für die Verwaltung persistenter Festplatten (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen
Importieren aus vCenter	**Manage Persistent Disks (Persistente Festplatten verwalten)** für den Ordner und **Manage Pool (Pool verwalten)** für den Pool.
Löschen einer Festplatte	**Manage Persistent Disks (Persistente Festplatten verwalten)** für die Festplatte.

Berechtigungen für die Verwaltung von Benutzern und Administratoren

Administratoren müssen über bestimmte Berechtigungen zur Verwaltung von Benutzern und Administratoren in View Administrator verfügen.

Tabelle 2-13 listet gängige Aufgaben für die Benutzer- und Administratorverwaltung sowie die erforderlichen Berechtigungen zur Ausführung der einzelnen Aufgaben auf. Benutzer werden auf der Seite **[Users and Groups (Benutzer und Gruppen)]** in View Administrator verwaltet. Administratoren werden in der globalen Administratorenansicht in View Administrator verwaltet.

Tabelle 2-13. Aufgaben und Berechtigungen für die Verwaltung von Benutzern und Administratoren

Aufgabe	Erforderliche Berechtigungen
Aktualisieren allgemeiner Benutzerinformationen	**Manage Global Configuration and Policies (Globale Konfiguration und Richtlinien verwalten)**
Senden von Nachrichten an Desktop-Benutzer	**Manage Remote Sessions (Remote-Sitzungen verwalten)** für den Desktop.
Hinzufügen von Administratorbenutzern oder -gruppen	**Manage Roles and Permissions (Rollen und Berechtigungen verwalten)**
Hinzufügen, Ändern oder Löschen von Administratorberechtigungen	**Manage Roles and Permissions (Rollen und Berechtigungen verwalten)**
Hinzufügen, Ändern oder Löschen von Administratorrollen	**Manage Roles and Permissions (Rollen und Berechtigungen verwalten)**

Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle

Administratoren müssen über bestimmte Berechtigungen zum Ausführen von allgemeinen Verwaltungsaufgaben und Befehlszeilenprogrammen verfügen.

Tabelle 2-14 zeigt die erforderlichen Berechtigungen, um allgemeine Verwaltungsaufgaben und Befehlszeilenprogramme auszuführen.

Tabelle 2-14. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle

Aufgabe	Erforderliche Berechtigungen
Hinzufügen oder Löschen eines Ordners	Administratorenrolle für den Stammordner.
Verwalten von ThinApp-Anwendungen und -Einstellungen in View Administrator	Administratorenrolle für den Stammordner.
Anzeigen und Ändern von View Transfer Server-Instanzen sowie des Transfer Server-Repositorys	Administratorenrolle für den Stammordner.
Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle (z.B. auf einem physischen System, einer eigenständigen virtuellen Maschine oder einem Terminalserver)	**Register Agent (Agent registrieren)**
Anzeigen oder Ändern von Konfigurationseinstellungen (Administratoreinstellungen ausgenommen) in View Administrator	**Manage Global Configuration and Policies (Globale Konfiguration und Richtlinien verwalten)**

Tabelle 2-14. Berechtigungen für allgemeine Verwaltungsaufgaben und -befehle (Fortsetzung)

Aufgabe	Erforderliche Berechtigungen
Ausführen aller PowerShell-Befehle und Befehlszeilenprogramme mit Ausnahme von `vdmadmin` und `vdmimport`.	**Direct Interaction (Direkte Interaktion)**
Verwenden der Befehle `vdmadmin` und `vdmimport`	Administratorenrolle für den Stammordner.
Verwenden des `vdmexport`-Befehls	Administratorenrolle (Lese- und Schreibzugriff oder nur Lesezugriff) für den Stammordner.

Empfohlene Vorgehensweisen für Administratorbenutzer und -gruppen

Um die Sicherheit und Verwaltbarkeit Ihrer View-Umgebung zu verbessern, sollten bei der Verwaltung von Administratorbenutzern und -gruppen empfohlene Vorgehensweisen befolgt werden.

- Da die Administratorrolle über sämtliche Berechtigungen verfügt, sollte diese Rolle einem einzelnen Benutzer oder einer eingeschränkten Anzahl an Benutzern zugewiesen werden.
- Wählen Sie zum Zuweisen der Administratorrolle einen lokalen Windows-Benutzer oder eine lokale Windows-Gruppe.
- Erstellen Sie für Administratoren neue Benutzergruppen. Vermeiden Sie die Verwendung von integrierten Windows-Gruppen oder anderen vorhandenen Gruppen, die möglicherweise zusätzliche Benutzer oder Gruppen enthalten.
- Vermeiden Sie beim Erstellen von Administratorbenutzern und -gruppen die Verwendung des Namens „Administrator“, da dieser offensichtlich und leicht zu erraten ist.
- Erstellen Sie separate Ordner für vertrauliche Desktops, um diese von anderen Elementen zu trennen. Delegieren Sie die Verwaltung dieser Ordner an eine eingeschränkte Anzahl an Benutzern.
- Erstellen Sie separate Administratoren, die globale Richtlinien und View-Konfigurationseinstellungen ändern können.

Vorbereiten nicht verwalteter Desktop-Quellen

3

Benutzer können auf View-Desktops zugreifen, die über nicht von vCenter Server verwaltete Maschinen bereitgestellt werden. Bei diesen nicht verwalteten Desktop-Quellen kann es sich um physische Computer, Terminalserver und virtuelle Maschinen handeln, die auf VMware Server und anderen Virtualisierungsplattformen ausgeführt werden. Sie müssen eine nicht verwaltete Desktop-Quelle vorbereiten, um Zugriff auf einen View-Desktop bereitzustellen.

Dieses Kapitel behandelt die folgenden Themen:

- „Vorbereiten einer nicht verwalteten Desktop-Quelle für die View-Desktop-Bereitstellung“, auf Seite 47
- „Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle“, auf Seite 48

Vorbereiten einer nicht verwalteten Desktop-Quelle für die View-Desktop-Bereitstellung

Zur Vorbereitung einer nicht verwalteten Desktop-Quelle für die View-Desktop-Bereitstellung müssen bestimmte Aufgaben ausgeführt werden.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf der nicht verwalteten Desktop-Quelle über Administratorberechtigungen verfügen.
- Um sicherzustellen, dass View-Desktop-Benutzer zur lokalen Gruppe **[Remote Desktop Users (Remotedesktopbenutzer)]** der nicht verwalteten Desktop-Quelle hinzugefügt werden, erstellen Sie eine eingeschränkte Gruppe **[Remote Desktop Users (Remotedesktopbenutzer)]** in Active Directory. Weitere Informationen finden Sie im Dokument *Installation von VMware View*.

Vorgehensweise

1. Schalten Sie die nicht verwaltete Desktop-Quelle ein und stellen Sie sicher, dass die View Connection Server-Instanz auf diese Quelle zugreifen kann.
2. Fügen Sie die nicht verwaltete Desktop-Quelle der Active Directory-Domäne für Ihre View-Desktops hinzu.
3. Konfigurieren Sie die Windows-Firewall so, dass Remote-Desktop-Verbindungen mit der nicht verwalteten Desktop-Quelle zulässig sind.

Weiter

Installieren Sie View Agent auf der nicht verwalteten Desktop-Quelle. Siehe „Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle“, auf Seite 48.

Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle

Sie müssen View Agent auf allen nicht verwalteten Desktop-Quellen installieren. View kann nicht verwaltete Desktop-Quellen nur dann verwalten, wenn View Agent installiert ist.

Um View Agent auf mehreren physischen Windows-Computern zu installieren, ohne auf Eingabeaufforderungen des Assistenten reagieren zu müssen, kann View Agent unbeaufsichtigt installiert werden. Siehe „Unbeaufsichtigte Installation von View Agent“, auf Seite 59.

Voraussetzungen

- Stellen Sie sicher, dass Sie auf der nicht verwalteten Desktop-Quelle über Administratorberechtigungen verfügen.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent für nicht verwaltete Desktop-Quellen vertraut. Siehe „Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Desktop-Quellen“, auf Seite 49.
- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der VMware View-Architektur*.
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/de/products/ herunter.

Vorgehensweise

1 Zum Starten des View Agent-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

Der Dateiname des Installationsprogramms lautet `VMware-viewagent-y.y.y-xxxxxx.exe` oder `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, wobei *y.y.y* die Versionsnummer und *xxxxxx* die Build-Nummer ist.

2 Stimmen Sie den Lizenzbedingungen von VMware zu.

3 Wählen Sie Ihre benutzerdefinierten Setup-Optionen.

4 Übernehmen oder ändern Sie den Zielordner.

5 Geben Sie im Textfeld **[Server]** den Hostnamen oder die IP-Adresse eines View Connection Server-Hosts ein.

Während der Installation registriert das Installationsprogramm die nicht verwaltete Desktop-Quelle bei dieser View Connection Server-Instanz. Nach der Registrierung können die angegebene View Connection Server-Instanz sowie alle zusätzlichen Instanzen in derselben View Connection Server-Gruppe mit der nicht verwalteten Desktop-Quelle kommunizieren.

6 Wählen Sie eine Authentifizierungsmethode zur Registrierung der nicht verwalteten Desktop-Quelle für die View Connection Server-Instanz.

Option	Aktion
Authentifizierung als aktuell angemeldeter Benutzer	Die Textfelder **[Username (Benutzername)]** und **[Password (Kennwort)]** sind deaktiviert und die Anmeldung an der View Connection Server-Instanz erfolgt über die aktuellen Anmeldeinformationen.
Angeben von Administratoranmeldeinformationen	In die Textfelder **[Username (Benutzername)]** and **[Password (Kennwort)]** müssen der Benutzername und das Kennwort eines View Connection Server-Administrators eingegeben werden.

7 Befolgen Sie die Anweisungen im View Agent-Installationsprogramm und schließen Sie die Installation ab.

8 Wenn Sie die USB-Umleitungsoption ausgewählt haben, starten Sie die nicht verwaltete Desktop-Quelle neu, um die USB-Unterstützung zu aktivieren.

   Es wird möglicherweise auch der Assistent **[Found New Hardware (Neue Hardware gefunden)]** gestartet. Befolgen Sie die Anweisungen des Assistenten zum Konfigurieren der Hardware, bevor Sie die nicht verwaltete Desktop-Quelle neu starten.

Der VMware View Agent-Dienst wird auf der nicht verwalteten Desktop-Quelle gestartet.

Wenn Windows Media Player nicht installiert ist, wird die MMR-Funktion (Multimedia Redirection) nicht vom View Agent-Installationsprogramm installiert. Wenn Sie Windows Media Player nach der Installation von View Agent installieren, können Sie die MMR-Funktion installieren, indem Sie das View Agent-Installationsprogramm erneut ausführen und die Option zum Reparieren wählen.

Weiter

Verwenden Sie die nicht verwaltete Desktop-Quelle, um einen View-Desktop zu erstellen. Siehe „Manuelle Desktop-Pools“, auf Seite 111.

Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Desktop-Quellen

Wenn Sie View Agent auf einer nicht verwalteten Desktop-Quelle installieren, können Sie bestimmte benutzerdefinierte Setup-Optionen auswählen.

Tabelle 3-1. Benutzerdefinierte Setup-Optionen für View Agent für nicht verwaltete Desktop-Quellen

Option	Beschreibung
USB Redirection (USB-Umleitung)	Gibt Benutzern Zugriff auf lokal verbundene USB-Geräte auf ihren Desktops. Die USB-Umleitung wird für Windows 2003 und Windows 2008 nicht unterstützt. **Hinweis** Sie können mithilfe von Gruppenrichtlinieneinstellungen die USB-Umleitung für spezifische Benutzer deaktivieren.
PCoIP Server (PCoIP-Server)	Ermöglicht Benutzern die Verbindungsherstellung mit dem View-Desktop über das PCoIP-Anzeigeprotokoll. **Hinweis** Wenn Sie unter Windows Vista die PCoIP-Server-Komponente installieren, wird die Windows-Gruppenrichtlinie **[Disable or enable software Secure Attention Sequence (Software-SAS deaktivieren oder aktivieren)]** aktiviert und auf **[Services (Dienste)]** und **[Ease of Access applications (Anwendungen für die erleichterte Bedienung)]** gesetzt. Wenn Sie diese Einstellung ändern, funktioniert SSO nicht mehr ordnungsgemäß.
PCoIP Smartcard (PCoIP-Smartcard)	Ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden.

Erstellen und Vorbereiten virtueller Maschinen

4

Sie können über vCenter Server verwaltete virtuelle Maschinen dazu verwenden, um View-Desktops zu provisionieren und bereitzustellen. Sie können eine virtuelle Maschine, die von vCenter Server verwaltet wird, als Vorlage für einen automatisierten Pool, für ein übergeordnetes Element für einen Linked-Clone-Pool oder für eine Desktop-Quelle in einem manuellen Pool verwenden. Sie müssen virtuelle Maschinen vorbereiten, um den Zugriff auf einen View-Desktop bereitzustellen.

Dieses Kapitel behandelt die folgenden Themen:

- „Erstellen virtueller Maschinen für die View-Desktop-Bereitstellung“, auf Seite 51
- „Installieren von View Agent auf einer virtuellen Maschine“, auf Seite 57
- „Unbeaufsichtigte Installation von View Agent“, auf Seite 59
- „Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent“, auf Seite 64
- „Optimieren der Leistung des Windows-Gastbetriebssystems“, auf Seite 65
- „Optimieren der Leistung des Windows 7-Gastbetriebssystems“, auf Seite 66
- „Optimieren von Windows 7 für Linked-Clone-Desktops“, auf Seite 66
- „Vorbereiten virtueller Maschinen für View Composer“, auf Seite 75
- „Erstellen von Vorlagen virtueller Maschinen“, auf Seite 81
- „Erstellen von Anpassungsspezifikationen“, auf Seite 81

Erstellen virtueller Maschinen für die View-Desktop-Bereitstellung

Mit der ersten virtuellen Maschine wird ein virtuelles Hardwareprofil und ein Betriebssystem eingerichtet, die für die schnelle Bereitstellung von View-Desktops verwendet werden.

1 Erstellen einer virtuellen Maschine für die View-Desktop-Bereitstellung auf Seite 52

Verwenden Sie vSphere Client zum Erstellen virtueller Maschinen in vCenter Server für View-Desktops.

2 Installieren eines Gastbetriebssystems auf Seite 54

Nachdem Sie eine virtuelle Maschine erstellt haben, müssen Sie ein Gastbetriebssystem installieren.

3 Vorbereiten eines Gastbetriebssystems für die View-Desktop-Bereitstellung auf Seite 55

Sie müssen bestimmte Aufgaben durchführen, um ein Gastbetriebssystem für die View-Desktop-Bereitstellung vorzubereiten.

Erstellen einer virtuellen Maschine für die View-Desktop-Bereitstellung

Verwenden Sie vSphere Client zum Erstellen virtueller Maschinen in vCenter Server für View-Desktops.

Voraussetzungen

- Laden Sie eine ISO-Image-Datei des Gastbetriebssystems in einen Datenspeicher auf Ihren ESX-Server hoch.
- Machen Sie sich mit den benutzerdefinierten Konfigurationsparametern für virtuelle Maschinen vertraut. Siehe „Benutzerdefinierte Konfigurationsparameter für die virtuelle Maschine“, auf Seite 52.

Vorgehensweise

1 Melden Sie sich in vSphere Client am vCenter Server-System an.

2 Wählen Sie **[File (Datei)] > [New (Neu)] > [Virtual Machine (Virtuelle Maschine)]**, um den Assistenten für neue virtuelle Maschinen zu starten.

3 Wählen Sie **[Custom (Benutzerdefiniert)]** aus und konfigurieren Sie benutzerdefinierte Konfigurationsparameter.

4 Wählen Sie **[Edit the virtual machine settings before completion (Einstellungen virtueller Maschinen vor Abschluss bearbeiten)]** aus und klicken Sie auf **[Continue (Weiter)]**, um die Hardwareeinstellungen zu konfigurieren.

   a Fügen Sie ein CD-/DVD-Laufwerk hinzu, legen Sie den Medientyp auf die Verwendung einer ISO-Image-Datei fest, wählen Sie das ISO-Image des Gastbetriebssystems, das Sie in Ihren Datenspeicher hochgeladen haben, und wählen Sie **[Connect at power on (Beim Einschalten verbinden)]**.

   b Wenn Sie ein Windows XP-Gastbetriebssystem installieren, fügen Sie ein Diskettenlaufwerk hinzu und legen Sie **[Device Type (Gerätetyp)]** auf **[Client Device (Clientgerät)]** fest.

   c Legen Sie **[Power-on Boot Delay (Startverzögerung nach dem Einschalten)]** auf 10.000 Millisekunden fest.

5 Klicken Sie auf **[Finish (Fertig stellen)]**, um die virtuelle Maschine zu erstellen.

Weiter

Installieren Sie ein Gastbetriebssystem auf der virtuellen Maschine.

Benutzerdefinierte Konfigurationsparameter für die virtuelle Maschine

Sie können benutzerdefinierte VM-Konfigurationsparameter als grundlegende Einstellungen für das Erstellen virtueller Maschinen in Ihrer View-Desktop-Bereitstellung verwenden.

Wenn Sie View Administrator als View-Desktop-Manager zum Bereitstellen von Desktop-Pools verwenden, können Sie diese Einstellungen beim Bereitstellen vorlagenbasierter View-Desktops verwenden.

Tabelle 4-1. Benutzerdefinierte Konfigurationsparameter

Parameter	Beschreibung und Empfehlungen
Name and Location (Name und Speicherort)	Der Name und der Speicherort der virtuellen Maschine. Wenn Sie die virtuelle Maschine als Vorlage verwenden möchten, weisen Sie ihr einen allgemeinen Namen zu. Der Speicherort kann ein beliebiger Ordner in der Bestandsliste des Rechenzentrums sein.
Host/Cluster	Der ESX-Server oder der Cluster an Serverressourcen, auf dem die virtuelle Maschine ausgeführt wird. Wenn die virtuelle Maschine als Vorlage verwendet werden soll, gibt der Speicherort der ersten virtuellen Maschine nicht zwangsläufig an, wo sich die zukünftigen virtuellen Maschinen befinden, die anhand dieser Vorlage erstellt wurden.
Resource Pool (Ressourcen-Pool)	Wenn die physischen ESX-Serverressourcen in Ressourcenpools unterteilt werden, können Sie sie der virtuellen Maschine zuweisen.
Datastore (Datenspeicher)	Der Speicherort der mit der virtuellen Maschine verknüpften Dateien.
Hardware Machine Version (Hardwareversion für die Maschine)	Wenn Sie die virtuelle Maschine auf einem ESXi 5.0 oder einem neueren Host oder Cluster erstellen, können Sie zwischen der virtuellen Hardwareversion 8 oder 7 wählen. Version 8 bietet dabei erweiterte Funktionalität für die virtuelle Maschine. Für Desktops, die im lokalen Modus ausgeführt werden, müssen Sie virtuelle Maschinen erstellen, die Hardwareversion 7 verwenden. Virtuelle Maschinen, die Hardwareversion 8 verwenden, können nicht für eine Verwendung im lokalen Modus ausgecheckt werden. Ist die Version des Hosts oder Clusters ESX/ESXi 4.0 oder eine neuere Version, können Sie nur die virtuelle Hardwareversion 7 auswählen.
Guest Operating System (Gastbetriebssystem)	Die Art des Betriebssystems, das Sie auf der virtuellen Maschine installieren.
CPUs	Die Anzahl an virtuellen Prozessoren in der virtuellen Maschine. Für die meisten Gastbetriebssysteme ist ein einzelner Prozessor ausreichend.
Memory (Arbeitsspeicher)	Die Arbeitsspeichergröße, die der virtuellen Maschine zugewiesen wird. In den meisten Fällen reicht 512 MB aus.

Tabelle 4-1. Benutzerdefinierte Konfigurationsparameter (Fortsetzung)

Parameter	Beschreibung und Empfehlungen
`Network (Netzwerk)`	Die Anzahl an virtuellen Netzwerkkarten (Network Interface Cards, NICs) in der virtuellen Maschine. Eine Netzwerkkarte reicht im Allgemeinen aus. Der Netzwerkname sollte in allen virtuellen Infrastrukturen konsistent sein. Ein falscher Netzwerkname in einer Vorlage kann zu Fehlern während der Anpassungsphasen der Instanz führen. Wenn Sie View Agent auf einer virtuellen Maschine installieren, die mehr als eine Netzwerkkarte besitzt, müssen Sie das von View Agent verwendete Subnetz konfigurieren. Siehe „Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent“, auf Seite 64 . **Wichtig** Für Betriebssysteme mit Windows 7 und Windows Vista müssen Sie den Netzwerkadapter „VMXNET 3“ auswählen. Die Verwendung des standardmäßigen E1000-Adapters kann zu Zeitüberschreitungsfehlern bei der Anpassung auf virtuellen Maschinen führen. Zur Verwendung des VMXNET 3-Adapters müssen Sie einen Microsoft-Hotfix-Patch installieren: ■ Für Windows 7 SP1: http://support.microsoft.com/kb/2550978 ■ Für Windows 7-Versionen vor SP1: http://support.microsoft.com/kb/2344941
`SCSI Controller (SCSI-Controller)`	Der Typ des SCSI-Adapters, der mit der virtuellen Maschine verwendet wird. Für die Gastbetriebssysteme Windows 7 und Windows XP sollten Sie den LSI Logic-Adapter angeben. Der LSI Logic-Adapter zeigt eine bessere Leistung und arbeitet mit generischen SCSI-Geräten besser zusammen. LSI Logic SAS ist nur für virtuelle Maschinen mit der Hardwareversion 7 verfügbar. **Hinweis** Windows XP umfasst keinen Treiber für den LSI Logic-Adapter. Sie müssen den Treiber von der LSI Logic-Website herunterladen.
`Select a Disk (Festplatte auswählen)`	Die Festplatte zur Verwendung mit der virtuellen Maschine. Erstellen Sie eine neue virtuelle Festplatte basierend auf der Größe des lokalen Speichers, den Sie jedem Benutzer zuweisen möchten. Berücksichtigen Sie ausreichend Speicherplatz für die Betriebssysteminstallation, Patches sowie lokal installierten Anwendungen. Um den Bedarf an Speicherplatz und die Verwaltung lokaler Daten zu reduzieren, wird empfohlen, die Informationen, das Profil und die Dokumente des Benutzers statt auf eine lokale Festplatte auf freigegebene Netzwerke zu speichern.

Installieren eines Gastbetriebssystems

Nachdem Sie eine virtuelle Maschine erstellt haben, müssen Sie ein Gastbetriebssystem installieren.

Voraussetzungen

- Stellen Sie sicher, dass sich eine ISO-Image-Datei des Gastbetriebssystems in einen Datenspeicher auf Ihren ESX-Server befindet.
- Vergewissern Sie sich, dass das CD-/DVD-Laufwerk in der virtuellen Maschine auf die ISO-Image-Datei des Gastbetriebssystems weist und dass das CD-/DVD-Laufwerk für die Verbindung beim Einschalten konfiguriert ist.

- Wenn Sie Windows XP installieren und den LSI Logic-Adapter für die virtuelle Maschine ausgewählt haben, laden Sie den Treiber für den LSI20320-R-Controller von der LSI Logic-Website herunter, erstellen Sie eine Disketten-Image-Datei (`.flp`), die den Treiber enthält, und laden Sie die Datei in einen Datenspeicher auf Ihrem ESX-Server hoch.

Vorgehensweise

1 Melden Sie sich in vSphere Client am vCenter Server-System an, auf dem sich die virtuelle Maschine befindet.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **[Power (Einschalten/Ausschalten)]** und **[Power On (Einschalten)]** aus, um die virtuelle Maschine zu starten.

Da Sie das CD-/DVD-Laufwerk so konfiguriert haben, dass es auf das ISO-Image weist und beim Einschalten verbunden wird, startet die Installation des Gastbetriebssystems automatisch.

3 Klicken Sie auf die Registerkarte **[Console (Konsole)]** und folgen Sie den Installationsanweisungen des Betriebssystemanbieters.

4 Wenn Sie Windows XP installieren und den LSI Logic-Adapter für die virtuelle Maschine ausgewählt haben, installieren Sie den LSI Logic-Treiber während des Windows-Setups.

   a Drücken Sie F6, um zusätzliche SCSI-Treiber auszuwählen.

   b Geben Sie **S** ein, um ein zusätzliches Gerät anzugeben.

   c Klicken Sie in der vSphere Client-Symbolleiste auf **[Connect Floppy (Diskette verbinden)]** , um die Diskettenimagedatei des LSI Logic-Treibers (`.flp`) auszuwählen.

   d Kehren Sie zum Windows-Installationsbildschirm zurück und drücken Sie die Eingabetaste, um mit dem Windows-Installationsvorgang fortzufahren.

   e Wenn der Windows-Installationsvorgang abgeschlossen wurde, trennen Sie die Verbindung zum virtuellen Diskettenlaufwerk.

5 Wenn Sie Windows 7 installieren, aktivieren Sie Windows online.

Weiter

Bereiten Sie das Gastbetriebssystem für die View-Desktop-Bereitstellung vor.

Vorbereiten eines Gastbetriebssystems für die View-Desktop-Bereitstellung

Sie müssen bestimmte Aufgaben durchführen, um ein Gastbetriebssystem für die View-Desktop-Bereitstellung vorzubereiten.

Voraussetzungen

- Erstellen Sie eine virtuelle Maschine und installieren Sie ein Gastbetriebssystem.
- Konfigurieren Sie einen Active Directory-Domänencontroller für Ihre View-Desktops. Weitere Informationen finden Sie im Dokument *Installation von VMware View*.
- Um sicherzustellen, dass View-Desktop-Benutzer zur lokalen Gruppe **[Remote Desktop Users (Remote-Desktop-Benutzer)]** der virtuellen Maschine hinzugefügt werden, erstellen Sie eine eingeschränkte Gruppe **[Remote Desktop Users (Remote-Desktop-Benutzer)]** in Active Directory. Weitere Informationen finden Sie im Dokument *Installation von VMware View*.
- Stellen Sie sicher, dass die Remote-Desktop-Dienste, in Windows XP-Systemen als „Terminaldienste“ bezeichnet, auf der virtuellen Maschine gestartet werden. Die Remote-Desktop-Dienste sind erforderlich für die Installation von View Agent, SSO und andere View-Vorgänge. Sie können den RDP-Zugriff auf Ihre View-Desktops durch Konfiguration der Desktop-Pool-Einstellungen und Gruppenrichtlinieneinstellungen deaktivieren. Siehe „Verhindern vom Zugriff auf View-Desktops durch RDP“, auf Seite 131.

- Stellen Sie sicher, dass Sie auf dem Gastbetriebssystem über Administratorberechtigungen verfügen.

Vorgehensweise

1 Melden Sie sich in vSphere Client am vCenter Server-System an, auf dem sich die virtuelle Maschine befindet.

2 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **[Power (Einschalten/Ausschalten)]** und **[Power On (Einschalten)]** aus, um die virtuelle Maschine zu starten.

3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, wählen Sie **[Guest (Gast)]** und **[Install/Upgrade VMware Tools (VMware Tools installieren/aktualisieren)]** aus, um die aktuelle Version von VMware Tools zu installieren.

4 Verwenden Sie die VMware Tools-Funktion zur Uhrzeitsynchronisierung um sicherzustellen, dass die virtuelle Maschine mit ESX synchronisiert ist.

   ESX muss mit einer externen NTP-Quelle synchronisiert werden, beispielsweise mit derselben Uhrzeitquelle wie Active Directory.

   Deaktivieren Sie andere Uhrzeitsynchronisierungsmechanismen wie z. B. den Windows-Zeitdienst.

   Die VMware Tools-Online-Hilfe stellt Informationen zum Konfigurieren der Uhrzeitsynchronisierung zwischen Gast und Host bereit.

5 Installieren Sie Service Packs und Updates.

6 Installieren Sie eine Antivirensoftware.

7 Installieren Sie weitere Anwendungen und Software, z.B. Windows Media Player, wenn Sie MMR verwenden, sowie Smartcard-Treiber, wenn Sie die Smartcard-Authentifizierung verwenden.

   In Windows XP-Systemen müssen alle Drittanbieter- und Softwareanwendungen (außer Microsoft .NET Framework) vor der Installation von View Agent installiert werden.

   WICHTIG Wenn Sie Microsoft .NET Framework installieren möchten, müssen Sie die Installation nach der Installation von View Agent durchführen.

8 Wenn View-Clients sich über das PCoIP-Anzeigeprotokoll mit der virtuellen Maschine verbinden, legen Sie die Energieoption **[Turn off the display (Anzeige deaktivieren)]** auf **[Never (Nie)]** fest.

   Wenn Sie diese Einstellung nicht deaktivieren, verbleibt die Anzeige bei Aktivierung des Energiesparmodus im letzten Status und scheint nicht mehr zu reagieren.

9 Wenn in Ihrer Netzwerkumgebung ein Proxy-Server verwendet wird, konfigurieren Sie die Proxy-Einstellungen für das Netzwerk.

10 Konfigurieren Sie die Eigenschaften für Netzwerkverbindungen.

   a Weisen Sie eine statische IP-Adresse zu oder geben Sie eine IP-Adresse an, die durch einen DHCP-Server vergeben wurde.

      View bietet keine Unterstützung für verbindungslokale Adressen (169.254.x.x) für View-Desktops.

   b Legen Sie die bevorzugte und alternative DNS-Serveradressen auf Ihre Active Directory-Serveradresse fest.

11 Fügen Sie die virtuelle Maschine der Active Directory-Domäne für Ihre View-Desktops hinzu.

   Eine übergeordnete virtuelle Maschine, die Sie für View Composer verwenden, muss entweder zu derselben Active Directory-Domäne wie die Domäne gehören, mit der sich die Linked-Clone-Desktops verbinden, oder sie muss Mitglied der lokalen ARBEITSGRUPPE sein.

12 Konfigurieren Sie die Windows-Firewall so, dass Remote-Desktop-Verbindungen mit der virtuellen Maschine zulässig sind.

13 (Optional) Deaktivieren Sie Hotplug-PCI-Geräte.

Dieser Schritt verhindert, dass Benutzer versehentlich das virtuelle Netzwerkgerät (vNIC) von der virtuellen Maschine trennen.

14 (Optional) Konfigurieren Sie Skripte für die Benutzeranpassung.

Weiter

Installieren Sie View Agent. Siehe „Installieren von View Agent auf einer virtuellen Maschine“, auf Seite 57.

Installieren von View Agent auf einer virtuellen Maschine

Sie müssen View Agent installieren, damit View Connection Server mit den über vCenter Server verwalteten virtuellen Maschinen kommunizieren kann. Installieren Sie View Agent auf allen virtuellen Maschinen, die Sie als Vorlage für automatisierte Desktop-Pools, übergeordnete Elemente für Linked-Clone-Desktop-Pools und Desktop-Quellen in manuellen Desktop-Pools verwenden.

Um View Agent auf mehreren virtuellen Windows-Maschinen zu installieren, ohne auf Eingabeaufforderungen des Assistenten reagieren zu müssen, kann View Agent unbeaufsichtigt installiert werden. Siehe „Unbeaufsichtigte Installation von View Agent“, auf Seite 59.

Voraussetzungen

- Bereiten Sie das Gastbetriebssystem für die View-Desktop-Bereitstellung vor. Siehe „Vorbereiten eines Gastbetriebssystems für die View-Desktop-Bereitstellung“, auf Seite 55.
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/de/products/ herunter.
- Stellen Sie sicher, dass Sie auf der virtuellen Maschine über Administratorberechtigungen verfügen.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent vertraut. Siehe „Benutzerdefinierte Setup-Optionen für View Agent“, auf Seite 58.
- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der VMware View-Architektur*.
- Wenn Sie die benutzerdefinierte Setup-Option für View Composer Agent auswählen, stellen Sie sicher, dass Sie über eine Lizenz zur Verwendung von View Composer verfügen.

Vorgehensweise

1 Zum Starten des View Agent-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

Der Dateiname des Installationsprogramms lautet `VMware-viewagent-y.y.y-xxxxxx.exe` oder `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, wobei *y.y.y* die Versionsnummer und *xxxxxx* die Build-Nummer ist.

2 Stimmen Sie den Lizenzbedingungen von VMware zu.

3 Wählen Sie Ihre benutzerdefinierten Setup-Optionen.

Wählen Sie zum Bereitstellen von Linked-Clone-Desktops die Option **[View Composer Agent]** aus.

4 Übernehmen oder ändern Sie den Zielordner.

5 Befolgen Sie die Anweisungen im View Agent-Installationsprogramm und schließen Sie die Installation ab.

HINWEIS Wenn Sie während der Vorbereitung des Gastbetriebssystems nicht die Remote-Desktop-Unterstützung aktiviert haben, werden Sie nun vom View Agent-Installationsprogramm aufgefordert, dies nachzuholen. Wenn Sie die Remote-Desktop-Unterstützung während der View Agent-Installation nicht aktivieren, müssen Sie die Aktivierung nach Abschluss der Installation manuell vornehmen.

6 Wenn Sie die USB-Umleitungsoption ausgewählt haben, starten Sie die virtuelle Maschine neu, um die USB-Unterstützung zu aktivieren.

Es wird möglicherweise auch der Assistent **[Found New Hardware (Neue Hardware gefunden)]** gestartet. Befolgen Sie die Anweisungen des Assistenten zum Konfigurieren der Hardware, bevor Sie die virtuelle Maschine neu starten.

Der VMware View Agent-Dienst wird auf der virtuellen Maschine gestartet.

Wenn Sie die Option **[View Composer Agent]** ausgewählt haben, wird der VMware View Composer Guest Agent Server-Dienst auf der virtuellen Maschine gestartet.

Wenn Windows Media Player nicht installiert ist, wird die MMR-Funktion (Multimedia Redirection) nicht vom View Agent-Installationsprogramm installiert. Wenn Sie Windows Media Player nach der Installation von View Agent installieren, können Sie die MMR-Funktion installieren, indem Sie das View Agent-Installationsprogramm erneut ausführen und die Option zum Reparieren wählen.

Weiter

Wenn die virtuelle Maschine über mehrere Netzwerkkarten verfügt, konfigurieren Sie das Subnetz, das View Agent verwendet. Siehe „Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent“, auf Seite 64.

Benutzerdefinierte Setup-Optionen für View Agent

Wenn Sie View Agent auf einer virtuellen Maschine installieren, können Sie benutzerdefinierte Setup-Optionen auswählen.

Tabelle 4-2. Benutzerdefinierte Setup-Optionen für View Agent

Option	Beschreibung
USB Redirection (USB-Umleitung)	Gibt Benutzern Zugriff auf lokal verbundene USB-Geräte auf ihren Desktops. Windows 2000 bietet keine Unterstützung für die USB-Umleitung. **HINWEIS** Sie können mithilfe von Gruppenrichtlinieneinstellungen die USB-Umleitung für spezifische Benutzer deaktivieren.
View Composer Agent	View Agent wird auf den Linked-Clone-Desktops ausgeführt, die von dieser virtuellen Maschine bereitgestellt werden.
Virtual Printing (Virtuelle Druckfunktion)	Benutzer können mit einem beliebigen Drucker drucken, der auf ihren Windows-Clientcomputern zur Verfügung steht. Benutzer müssen keine zusätzlichen Treiber auf ihren Desktops installieren.

Tabelle 4-2. Benutzerdefinierte Setup-Optionen für View Agent (Fortsetzung)

Option	Beschreibung
PCoIP Server (PCoIP-Server)	Ermöglicht Benutzern die Verbindungsherstellung mit dem View-Desktop über das PCoIP-Anzeigeprotokoll. Wenn Sie die Funktion **[PCoIP Server (PCoIP-Server)]** installieren, wird auf Windows 7- und Windows Vista-Desktops der Energiesparmodus und auf Windows XP-Desktops der Standbymodus deaktiviert. Wenn ein Benutzer zum Menü für die Energieoptionen oder das Abschalten wechselt, wird der Energiesparmodus oder Standbymodus als inaktiv angezeigt. Desktops wechseln nach der standardmäßig angegebenen Leerlaufzeit nicht in den Energiespar- oder Standbymodus. Desktops verbleiben im aktiven Modus. **Hinweis** Wenn Sie unter Windows Vista die Funktion **[PCoIP Server (PCoIP-Server)]** installieren, wird die Windows-Gruppenrichtlinie **[Disable or enable software Secure Attention Sequence (Software-SAS deaktivieren oder aktivieren)]** aktiviert und auf **[Services and Ease of Access applications (Dienste und Anwendungen für die erleichterte Bedienung)]** gesetzt. Wenn Sie diese Einstellung ändern, funktioniert SSO nicht mehr ordnungsgemäß.
PCoIP Smartcard (PCoIP-Smartcard)	Ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden.
View Persona-Verwaltung	Synchronisiert das Benutzerprofil auf dem lokalen Desktop mit einem Remote-Profil-Repository, damit die Benutzer immer Zugriff auf ihre Profile haben, wenn sie sich bei einem Desktop anmelden.

Unbeaufsichtigte Installation von View Agent

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, View Agent auf mehreren virtuellen Windows-Maschinen oder physischen Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Bereiten Sie das Gastbetriebssystem für die View-Desktop-Bereitstellung vor. Siehe „Vorbereiten eines Gastbetriebssystems für die View-Desktop-Bereitstellung“, auf Seite 55.
- Laden Sie die View Agent-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/de/products/ herunter.

  Der Dateiname des Installationsprogramms lautet `VMware-viewagent-y.y.y-xxxxxx.exe` oder `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, wobei *y.y.y* die Versionsnummer und *xxxxxx* die Build-Nummer ist.
- Stellen Sie sicher, dass Sie auf der virtuellen Maschine oder auf dem physischen Computer über Administratorberechtigungen verfügen.
- Machen Sie sich mit den benutzerdefinierten Setup-Optionen für View Agent vertraut. Siehe „Benutzerdefinierte Setup-Optionen für View Agent“, auf Seite 58.
- Wenn Sie die benutzerdefinierte Setup-Option für View Composer Agent auswählen, stellen Sie sicher, dass Sie über eine Lizenz zur Verwendung von View Composer verfügen.

- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 60.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation von View Agent vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation von View Agent“, auf Seite 62.
- Machen Sie sich mit den TCP-Ports vertraut, die das View Agent-Installationsprogramm in der Firewall öffnet. Weitere Informationen finden Sie im Dokument *Planung der VMware View-Architektur*.

Vorgehensweise

1 Öffnen Sie auf der virtuellen Maschine oder auf einem physischen Computer eine Windows-Eingabeaufforderung.

2 Geben Sie den Installationsbefehl in einer Zeile ein.

In diesem Beispiel wird View Agent in einer virtuellen Maschine installiert, die von vCenter Server verwaltet wird. Das Installationsprogramm konfiguriert die benutzerdefinierten Setup-Optionen für PCoIP, View Composer Agent, die Funktion für den virtuellen Druck und die USB-Umleitung.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 ADDLOCAL=Core,PCoIP,SVI-
Agent,ThinPrint,USB"
```

In diesem Beispiel werden View Agent auf einem nicht verwalteten Computer installiert und der Desktop bei dem angegebenen View Connection Server `cs1.companydomain.com` registriert. Mit dem Installationsprogramm wird SSO, die Funktion für den virtuellen Druck und die benutzerdefinierten Setup-Optionen für die USB-Umleitung konfiguriert.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0 VDM_SERVER_NAME=cs1.compa-
nydomain.com VDM_SERVER_USERNAME=admin.companydomain.com VDM_SERVER_PASSWORD=secret ADDLO-
CAL=Core,ThinPrint,USB"
```

Der VMware View Agent-Dienst wird auf der virtuellen Maschine gestartet.

Wenn Sie die Option **[View Composer Agent]** ausgewählt haben, wird der VMware View Composer Guest Agent Server-Dienst auf der virtuellen Maschine gestartet.

Wenn Windows Media Player nicht installiert ist, wird die MMR-Funktion (Multimedia Redirection) nicht vom View Agent-Installationsprogramm installiert. Wenn Sie Windows Media Player nach der Installation von View Agent installieren, können Sie die MMR-Funktion installieren, indem Sie das View Agent-Installationsprogramm erneut ausführen und die Option zum Reparieren wählen.

Weiter

Wenn die virtuelle Maschine über mehrere Netzwerkkarten verfügt, konfigurieren Sie das Subnetz, das View Agent verwendet. Siehe „Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent“, auf Seite 64.

Microsoft Windows Installer-Befehlszeilenoptionen

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen.

Weitere Informationen zum Microsoft Windows Installer (MSI) finden Sie auf der Microsoft-Website. Informationen zu MSI-Befehlszeilenoptionen erhalten Sie, wenn Sie auf der Microsoft Developer Network (MSDN) Library-Website nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

Sie müssen in die Befehlszeile Befehlszeilenoptionen eingeben, mit denen das Bootstrap-Programm des Installationsprogramms gesteuert wird.

Tabelle 4-3. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente

Option	Beschreibung
`/s`	Deaktiviert den Bootstrap-Begrüßungsbildschirm und das Dialogfeld für das Extrahieren, sodass keine interaktiven Dialogfeld angezeigt werden. Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` Die Option `/s` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.
`/v" MSI-Befehlszeilenoptionen"`	Weist das Installationsprogramm an, die in doppelte Anführungszeichen eingeschlossene Zeichenfolge, die an der Befehlszeile eingegeben wurde, als MSI-Optionssatz auszuwerten. Sie müssen die Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Platzieren Sie ein doppeltes Anführungszeichen nach `/v` und am Ende der Befehlszeile. Beispiel: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"Befehlszeilenoptionen"` Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält. Beispiel: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"Befehlszeilenoptionen INSTALLDIR=""d:\abc\my folder"""` In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen. Die Option `/v"Befehlszeilenoptionen"` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.

Sie steuern den verbleibenden Teil einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaften an das MSI-Installationsprogramm (`msiexec.exe`) übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

Tabelle 4-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
`/qn`	Weist das MSI-Installationsprogramm an, keine Seiten des Installations-Assistenten anzuzeigen. Angenommen, Sie möchten View Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` Alternativ können Sie die Option `/qb` verwenden, um die Assistentenseiten in einer nicht interaktiven, automatisierten Installation anzuzeigen. Im Verlauf der Installation werden die Assistentenseiten angezeigt, eine Eingabe ist jedoch nicht möglich. Die Option `/qn` oder `/qb` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.
`INSTALLDIR`	Gibt einen alternativen Installationspfad für die View-Komponente an. Verwenden Sie das Format *INSTALLDIR=Pfad*, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten. Diese MSI-Eigenschaft ist optional.

Tabelle 4-4. MSI-Befehlszeilenoptionen und MSI-Eigenschaften (Fortsetzung)

MSI-Option oder -Eigenschaft	Beschreibung
ADDLOCAL	Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das View-Installationsprogramm Auswahloptionen für das benutzerdefinierte Setup an. Mithilfe der MSI-Eigenschaft ADDLOCAL können Sie diese Setup-Optionen an der Befehlszeile angeben. Um alle verfügbaren Optionen für ein benutzerdefiniertes Setup zu installieren, geben Sie ADDLOCAL=ALL ein. Beispiel: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Wenn Sie die MSI-Eigenschaft ADDLOCAL nicht verwenden, werden die standardmäßigen Setup-Optionen installiert. Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format *ADDLOCAL=Wert,Wert,Wert...*. Angenommen, Sie möchten View Agent mit den View Composer Agent- und PCoIP-Funktionen in einem Gastbetriebssystem installieren: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **Hinweis** Die Funktion Core ist in View Agent erforderlich. Diese MSI-Eigenschaft ist optional.
REBOOT	Sie können die Option REBOOT=ReallySuppress verwenden, um zuzulassen, dass Systemkonfigurationsaufgaben vor einem Neustart des Systems ausgeführt werden dürfen. Diese MSI-Eigenschaft ist optional.
/l*v *Protokolldatei*	Schreibt Protokollierungsinformationen in die angegebene Protokolldatei. Hierbei ist eine ausführliche Ausgabe festgelegt. Beispiel: /l*v ""%TEMP%\vmmsi.log"" In diesem Beispiel wird eine ausführliche Protokolldatei ähnlich dem Protokoll generiert, das bei einer interaktiven Installation erstellt wird. Sie können mit dieser Option benutzerdefinierte Funktionen erfassen, die möglicherweise nur für Ihre Installation gelten. Sie können die protokollierten Informationen verwenden, um Installationsfunktionen in zukünftigen unbeaufsichtigten Installationen anzugeben. Die Option /l*v ist optional.

Eigenschaften für die unbeaufsichtigte Installation von View Agent

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation eines Sicherheitsservers über die Befehlszeile ausführen. Sie müssen hierbei das Format *EIGENSCHAFT=Wert* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 4-5 zeigt die Eigenschaften für eine unbeaufsichtigte Installation von View Agent, die Sie an der Befehlszeile verwenden können.

Tabelle 4-5. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Agent

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Agent-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles %\VMware\VMware View\Agent`
RDPCHOICE	Legt fest, ob RDP (Remote Desktop Protocol) auf dem Desktop aktiviert werden soll. Mit dem Wert 1 wird RDP aktiviert. Mit dem Wert 0 wird die RDP-Einstellung deaktiviert. Diese MSI-Eigenschaft ist optional.	1
VDM_VC_MANAGED_AGENT	Legt fest, ob vCenter Server die virtuelle Maschine verwaltet, auf der View Agent installiert ist. Mit dem Wert 1 wird der Desktop als von vCenter Server verwaltete virtuelle Maschine konfiguriert. Mit dem Wert 0 wird der Desktop ohne Verwaltung durch vCenter Server konfiguriert. Diese MSI-Eigenschaft ist erforderlich.	–
VDM_SERVER_NAME	Der Hostname oder die IP-Adresse des View Connection Server-Computers, auf dem das View Agent-Installationsprogramm einen nicht verwalteten Desktop registriert. Diese Eigenschaft gilt nur für nicht verwaltete Desktops. Beispiel: `VDM_SERVER_NAME=10.123.01.01` Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich. Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.	–
VDM_SERVER_USERNAME	Der Benutzername des Administrators auf dem View Connection Server-Computer. Diese MSI-Eigenschaft gilt nur für nicht verwaltete Desktops. Beispiel: `VDM_SERVER_USERNAME=admin.companydomain.com` Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich. Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.	–
VDM_SERVER_PASSWORD	Das Benutzerkennwort des View Connection Server-Administrators. Beispiel: `VDM_SERVER_PASSWORD=secret` Diese MSI-Eigenschaft ist für nicht verwaltete Desktops erforderlich. Verwenden Sie diese MSI-Eigenschaft nicht für VM-Desktops, die von vCenter Server verwaltet werden.	–

In einem Befehl für die unbeaufsichtigte Installation können Sie mit der MSI-Eigenschaft `ADDLOCAL=` benutzerdefinierte Funktionen angeben, die das View Agent-Installationsprogramm konfiguriert. Jede Funktion für die unbeaufsichtigte Installation entspricht einer benutzerdefinierten Setup-Option, die Sie während einer interaktiven Installation auswählen können.

Tabelle 4-6 zeigt die View Agent-Funktionen, die Sie an der Befehlszeile angeben können, sowie die entsprechenden benutzerdefinierten Setup-Optionen.

Tabelle 4-6. Funktionen für die unbeaufsichtigte View Agent-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option bei einer interaktiven Installation
Core. Wenn Sie mithilfe der MSI-Eigenschaft `ADDLOCAL=` einzelne Funktionen angeben, müssen Sie Core einschließen. Wenn Sie `ADDLOCAL=ALL` angeben, werden alle Funktionen, einschließlich Core, installiert.	– Bei einer interaktiven Installation werden die View Agent-Hauptfunktionen standardmäßig installiert.
SVIAgent	View Composer Agent
ThinPrint	Virtual Printing (Virtuelle Druckfunktion)
ThinPrintPCoIP	Virtual Printing with PCoIP (Virtueller Druck mit PCoIP)
PCoIP	PCoIP Protocol (PCoIP-Protokoll)
USB	USB Redirection (USB-Umleitung)
VPA	View Persona-Verwaltung
VmVideo	In einer interaktiven Installation ist diese Funktion keine separate benutzerdefinierte Einrichtungsoption.
VmwAudio	In einer interaktiven Installation ist diese Funktion keine separate benutzerdefinierte Einrichtungsoption.
SmartCard	In einer interaktiven Installation ist die SmartCard-Funktion keine separate benutzerdefinierte Einrichtungsoption.
VMCI	In einer interaktiven Installation ist die VMCI-Funktion keine separate benutzerdefinierte Einrichtungsoption.

Weitere Informationen zu den benutzerdefinierten Setup-Optionen finden Sie unter „Benutzerdefinierte Setup-Optionen für View Agent“, auf Seite 58.

Konfigurieren einer virtuellen Maschine mit mehreren Netzwerkkarten für View Agent

Wenn Sie View Agent auf einer virtuellen Maschine installieren, die mehr als eine Netzwerkkarte besitzt, müssen Sie das von View Agent verwendete Subnetz konfigurieren. Mit dem Subnetz wird festgelegt, welche Netzwerkadresse View Agent der View Connection Server-Instanz für Clientprotokollverbindungen bereitstellt.

Vorgehensweise

- Öffnen Sie auf der virtuellen Maschine, auf der View Agent installiert ist, eine Eingabeaufforderung, geben Sie **`regedit.exe`** ein und erstellen Sie einen Registrierungseintrag, um das Subnetz zu konfigurieren.

  Beispiel: **`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)`**

  In diesem Beispiel steht *n.n.n.n* für das TCP/IP-Subnetz und *m* für die Anzahl der Bits in der Subnetzmaske.

Optimieren der Leistung des Windows-Gastbetriebssystems

Sie können bestimmte Schritte ausführen, um die Leistung des Gastbetriebssystems für eine View-Desktop-Bereitstellung zu optimieren. Die Schritte gelten für alle Windows-Betriebssysteme. Alle genannten Schritte sind optional.

Es wird u. a. empfohlen, den Bildschirmschoner auszuschalten und keinen Ruhezustandstimer anzugeben. Möglicherweise verlangt Ihr Unternehmen die Verwendung eines Bildschirmschoners. So sorgt beispielsweise eine GPO-verwaltete Sicherheitsrichtlinie dafür, dass ein Desktop nach Ablauf einer bestimmten Zeit nach dem Starten des Bildschirmschoners gesperrt wird. Verwenden Sie in einem solchen Fall einen leeren Bildschirmschoner.

Voraussetzungen

Bereiten Sie ein Gastbetriebssystem für die View-Desktop-Bereitstellung vor.

Vorgehensweise

- Deaktivieren Sie alle nicht verwendeten Ports, beispielsweise COM1, COM2 und LPT.
- Passen Sie die Anzeigeeigenschaften an.
  a Wählen Sie ein Basisdesign.
  b Legen Sie den Hintergrund auf eine Volltonfarbe fest.
  c Legen Sie den Bildschirmschoner auf **[None (Keiner)]** fest.
  d Stellen Sie sicher, dass die Hardwarebeschleunigung aktiviert ist.
- Wählen Sie eine Betriebsoption mit hoher Leistung aus und legen Sie keinen Wechsel in den Energiesparmodus fest.
- Deaktivieren Sie den Indexdienst.

  Hinweis Die Indizierung verbessert die Suche, indem Dateien katalogisiert werden. Deaktivieren Sie diese Funktion nicht bei Benutzern, die die Suche häufig verwenden.
- Entfernen Sie Systemwiederherstellungspunkte, oder reduzieren Sie diese auf ein Mindestmaß.
- Deaktivieren Sie den Systemschutz für `C:\`.
- Deaktivieren Sie alle nicht benötigten Dienste.
- Legen Sie das Soundschema auf **[No Sounds (Keine Sounds)]** fest.
- Legen Sie die visuellen Effekte auf **[Adjust for best performance (Für optimale Leistung anpassen)]** fest.
- Öffnen Sie Windows Media Player und verwenden Sie die Standardeinstellungen.
- Deaktivieren Sie die automatische Computerwartung.
- Passen Sie die Leistungseinstellungen für eine optimale Leistung an.
- Löschen Sie alle versteckten Ordner für die Deinstallation unter `C:\Windows`, beispielsweise `$NtUninstallKB893756$`.
- Löschen Sie alle Ereignisprotokolle.
- Führen Sie eine Datenträgerbereinigung zum Entfernen temporärer Dateien durch, leeren Sie den Papierkorb und entfernen Sie Systemdateien und andere Elemente, die nicht mehr benötigt werden.
- Führen Sie eine Datenträgerdefragmentierung aus, um fragmentierte Daten neu anzuordnen.

Weiter

Führen Sie auf Windows 7-Gastbetriebssystemen zusätzliche Schritte zur Optimierung aus. Siehe „Optimieren der Leistung des Windows 7-Gastbetriebssystems“, auf Seite 66.

Optimieren der Leistung des Windows 7-Gastbetriebssystems

Sie können zusätzliche Schritte ausführen, um die Leistung des Windows 7-Gastbetriebssystems für eine View-Desktop-Bereitstellung zu optimieren. Alle genannten Schritte sind optional.

Voraussetzungen

Führen Sie die Schritte zur Leistungsoptimierung für das Gastbetriebssystem aus, die für alle Windows-Betriebssysteme gelten. Siehe „Optimieren der Leistung des Windows-Gastbetriebssystems“, auf Seite 65.

Vorgehensweise

1 Deinstallieren Sie Tablet PC-Komponenten – es sei denn, diese werden benötigt.

2 Deaktivieren Sie IPv6, sofern diese Funktion nicht benötigt wird.

3 Verwenden Sie das Dateisystemprogramm (`fsutil`), um die Nachverfolgung des letzten Zugriffszeitpunkts für eine Datei zu deaktivieren.

   Beispiel: `fsutil behavior set disablelastaccess 1`

4 Starten Sie den Registrierungs-Editor (`regedit.exe`) und ändern Sie den REG_WORD-Eintrag **[TimeOutValue]** in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk` auf **`0x000000be(190)`**.

5 Fahren Sie das Gastbetriebssystem herunter und schalten Sie die virtuelle Maschine aus.

6 Ändern Sie die RAM-Einstellung für die Grafikkarte der virtuellen Maschine in 128 MB.

7 Schalten Sie die virtuelle Maschine ein.

Weiter

Siehe „Optimieren von Windows 7 für Linked-Clone-Desktops“, auf Seite 66 finden Sie Informationen dazu, wie Sie durch das Deaktivieren bestimmter Windows 7-Dienste und -Tasks das Wachstum von View Composer-Linked-Clone-Desktops verlangsamen können. Das Deaktivieren bestimmter Dienste und Tasks kann außerdem die Leistung vollständiger virtueller Maschinen verbessern.

Optimieren von Windows 7 für Linked-Clone-Desktops

Durch das Deaktivieren bestimmter Windows 7-Dienste und -Tasks können Sie das Wachstum von View Composer-Linked-Clone-Desktops verlangsamen. Das Deaktivieren bestimmter Dienste und Tasks kann außerdem die Leistung vollständiger virtueller Maschinen verbessern.

Vorteile der Deaktivierung von Windows 7-Diensten und -Tasks

Windows 7 plant die Ausführung von Diensten und Tasks, die verknüpfte View Composer-Klone anwachsen lassen können, selbst wenn die Linked-Clone-Desktops sich im Leerlauf befinden. Das inkrementelle Wachstum von Linked-Clone-Betriebssystemfestplatten kann die Speichereinsparungen zunichte machen, die Sie durch das Erstellen von Linked-Clone-Desktops erzielen. Sie können das Wachstum von Linked-Clone-Desktops verringern, indem Sie diese Windows 7-Dienste deaktivieren.

In Windows 7 werden verschiedene neu eingeführte Dienste und ältere Dienste, wie beispielsweise die Datenträgerdefragmentierung, zur standardmäßigen Ausführung geplant. Diese Dienste werden im Hintergrund ausgeführt, wenn Sie sie nicht deaktivieren.

Dienste, die sich auf das Wachstum der Betriebssystemfestplatte auswirken, erhöhen außerdem die Anzahl an E/A-Vorgängen pro Sekunde auf den virtuellen Windows 7-Maschinen. Durch das Deaktivieren dieser Dienste kann die Anzahl an E/A-Vorgängen pro Sekunde verringert und die Leistung auf vollständigen virtuellen Maschinen und verknüpften Klonen verbessert werden.

Das Deaktivieren bestimmter Dienste kann sich auch auf den Betriebssystemen Windows XP und Windows Vista positiv auswirken.

Die hier vorgestellten empfohlenen Vorgehensweisen zur Optimierung von Windows 7 gelten für die meisten Benutzerumgebungen. Sie müssen jedoch die Auswirkung der Deaktivierung einzelner Dienste auf Ihre Benutzer, Anwendungen und Desktops berücksichtigen. Bestimmte Dienste müssen möglicherweise ausgeführt werden.

Beispielsweise ist das Deaktivieren des Windows Update-Dienstes sinnvoll, wenn Sie Linked-Clone-Desktops aktualisieren und neu zusammenstellen. Bei einer Aktualisierung werden die Betriebssystemfestplatten im Zustand der letzten Snapshots wiederhergestellt, und alle automatischen Windows-Updates seit Erstellung des letzten Snapshots werden gelöscht. Bei einer Neuzusammenstellung werden die Betriebssystemfestplatten unter Verwendung eines neuen Snapshots erneut erstellt. Da dieser neue Snapshot die aktuellen Windows-Updates möglicherweise bereits umfasst, sind automatische Windows-Updates überflüssig.

Wenn Sie Aktualisierungen und Neuzusammenstellungen nicht regelmäßig ausführen, sollten Sie den Windows Update-Dienst möglicherweise weiterhin ausführen.

Überblick über Windows 7-Dienste und -Tasks, die zu einem Wachstum von verknüpften Klonen führen

Bestimmte Windows 7-Dienste und -Tasks können dazu führen, dass die Linked-Clone-Betriebssystemfestplatten inkrementell anwachsen, selbst wenn die Linked-Clone-Desktops sich im Leerlauf befinden. Wenn Sie diese Dienste und Tasks deaktivieren, können Sie das Wachstum der Betriebssystemfestplatten kontrollieren.

Dienste, die sich auf das Wachstum der Betriebssystemfestplatten auswirken, erzeugen auch eine höhere Anzahl an E/A-Vorgängen pro Sekunde auf den virtuellen Windows 7-Maschinen. Sie sollten auswerten, welche Vorteile eine Deaktivierung dieser Dienste auf vollständigen virtuellen Maschinen und verknüpften Klonen bietet.

Bevor Sie die Windows 7-Dienste deaktivieren, die in Tabelle 4-7gezeigt werden, führen Sie die Optimierungsschritte unter „Optimieren der Leistung des Windows-Gastbetriebssystems“, auf Seite 65 und „Optimieren der Leistung des Windows 7-Gastbetriebssystems“, auf Seite 66 aus.

Tabelle 4-7. Auswirkung von Windows 7-Diensten und -Tasks auf das Wachstum von Betriebssystemfestplatten und E/A-Vorgänge pro Sekunde, wenn das Betriebssystem sich im Leerlauf befindet

Dienst oder Task	Beschreibung	Standardhäufigkeit oder -start	Auswirkung auf Linked-Clone-Betriebssystemfestplatten	Auswirkung auf E/A-Vorgänge pro Sekunde	Dienst oder Task deaktivieren?
Windows-Ruhezustand	Versetzt das System in einen Zustand zur Energieeinsparung, indem offene Dokumente und Programme in einer Datei gespeichert werden, bevor der Computer ausgeschaltet wird. Die Datei wird erneut in den Arbeitsspeicher geladen, wenn der Computer neu gestartet wird, und es wird der Zustand vor Auslösung des Ruhezustands wiederhergestellt.	Ruhezustand ist in den Einstellungen des standardmäßigen Energiesparplans deaktiviert	Hoch. Standardmäßig entspricht die Größe der Datei für den Ruhezustand, `hiberfil.sys`, der des installierten Arbeitsspeichers auf der virtuellen Maschine. Diese Funktion betrifft alle Gastbetriebssysteme.	Hoch. Beim Auslösen des Ruhezustands erstellt das System die Datei `hiberfil.sys`, die so groß ist wie der installierte Arbeitsspeicher.	Ja. Der Ruhezustand bietet in einer virtuellen Umgebung keine Vorteile. Anweisungen finden Sie unter „Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine“, auf Seite 78..
Geplante Windows-Datenträgerdefragmentierung	Die Datenträgerdefragmentierung ist als Hintergrundprozess geplant.	Einmal pro Woche	Hoch. Wiederholte Defragmentierungsvorgänge können die Linked-Clone-Betriebssystemfestplatten um mehrere GB anwachsen lassen und verbessern den Festplattenzugriff auf verknüpfte Klone nur unwesentlich.	High (Hoch)	Ja.
Windows Update-Dienst	Sorgt für Ermittlung, Download und Installation von Updates für Windows und andere Programme.	Automatischer Start	Mittel bis hoch. Verursacht häufige Schreibvorgänge auf den Linked-Clone-Betriebssystemfestplatten, da häufig auf Updates geprüft wird. Die Auswirkung richtet sich nach den Updates, die heruntergeladen werden.	Mittel bis hoch	Ja, wenn Sie View Composer-Neuzusammenstellungen zum Installieren von Windows-Updates und Aktualisierungen dazu verwenden, um Betriebssystemfestplatten in den Zustand ihrer ursprünglichen Snapshots zurückzuversetzen.

Tabelle 4-7. Auswirkung von Windows 7-Diensten und -Tasks auf das Wachstum von Betriebssystemfestplatten und E/A-Vorgänge pro Sekunde, wenn das Betriebssystem sich im Leerlauf befindet (Fortsetzung)

Dienst oder Task	Beschreibung	Standardhäufigkeit oder -start	Auswirkung auf Linked-Clone-Betriebssystemfestplatten	Auswirkung auf E/A-Vorgänge pro Sekunde	Dienst oder Task deaktivieren?
Windows-Diagnoserichtliniendienst	Ermittlung, Fehlerbehebung und Lösung von Problemen in Windows-Komponenten. Wenn Sie diesen Dienst anhalten, ist eine Diagnose nicht länger möglich.	Automatischer Start	Mittel bis hoch. Der Dienst wird bei Bedarf gestartet. Die Häufigkeit von Schreibvorgängen variiert je nach Bedarf.	Gering bis mittel	Ja, wenn Sie die Diagnosetools auf den Desktops nicht benötigen.
Vorabruf/SuperFetch	Speichert spezifische Informationen zu ausgeführten Anwendungen, damit diese schneller gestartet werden. Diese Funktion wurde in Windows XP eingeführt.	Sie ist immer eingeschaltet, sofern Sie sie nicht deaktivieren.	Medium (Mittel) Führt regelmäßige Updates an den Layout- und Datenbankinformationen sowie einzelnen Dateien für den Vorabruf durch, die bei Bedarf generiert werden.	Medium (Mittel)	Ja, wenn die Startzeiten für Anwendungen auch nach dem Deaktivieren dieser Funktion akzeptabel sind.
Sicherung der Windows-Registrierung (`RegIdleBackup`)	Führt eine automatische Sicherung der Windows-Registrierung durch, wenn das System sich im Leerlauf befindet.	Alle 10 Tage um 12:00 Uhr	Mittel. Bei jeder Ausführung dieses Tasks werden Sicherungsdateien der Registrierung erstellt.	Mittel.	Ja. Es besteht keine Notwendigkeit zur Sicherung der Windows-Registrierung. Zum Wiederherstellen von Registrierungsdaten können Sie eine View Composer-Aktualisierung durchführen.
Systemwiederherstellung	Stellt das Windows-System in einem vorherigen, fehlerfreien Zustand wieder her.	Beim Start von Windows und anschließend einmal täglich	Gering bis mittel. Erfasst immer dann einen Systemwiederherstellungspunkt, wenn das System dies als erforderlich betrachtet. Wenn sich der verknüpfte Klon im Leerlauf befindet, ist der so entstehende Overhead gering.	Keine nennenswerte Auswirkung	Ja. Trotz geringer Auswirkung ist dieser Task überflüssig, wenn Sie Betriebssystemfestplatten mithilfe von View Composer in den Zustand ihrer ursprünglichen Snapshots zurückversetzen.

Tabelle 4-7. Auswirkung von Windows 7-Diensten und -Tasks auf das Wachstum von Betriebssystemfestplatten und E/A-Vorgänge pro Sekunde, wenn das Betriebssystem sich im Leerlauf befindet (Fortsetzung)

Dienst oder Task	Beschreibung	Standardhäufigkeit oder -start	Auswirkung auf Linked-Clone-Betriebssystemfestplatten	Auswirkung auf E/A-Vorgänge pro Sekunde	Dienst oder Task deaktivieren?
Windows Defender	Stellt Anti-Spyware-Funktionen bereit.	Beim Start von Windows. Führt einmal täglich eine Schnellprüfung durch. Vor jedem Scan wird auf Updates geprüft.	Mittel bis hoch. Führt Definitions-Updates, geplante Scans und Scans aus, die bei Bedarf gestartet werden.	Mittel bis hoch.	Ja, wenn eine andere Anti-Spyware-Software installiert ist.
Microsoft-Feeds-Synchronisierung (`msfeedssync.exe`)	Führt eine regelmäßige Aktualisierung der RSS-Feeds in Windows Internet Explorer 7 und 8 durch. Dieser Task aktualisiert RSS-Feeds, für die eine automatische RSS-Feed-Synchronisierung aktiviert wurde. Der Prozess erscheint nur im Windows Task Manager, wenn Internet Explorer 7 oder 8 ausgeführt wird.	Einmal täglich	Mittel. Wirkt sich auf das Wachstum von Betriebssystemfestplatten aus, wenn keine persistenten Festplatten konfiguriert sind. Sind persistente Festplatten konfiguriert, gelten die Auswirkungen für die persistenten Festplatten.	Medium (Mittel)	Ja, wenn Ihre Benutzer keine automatischen RSS-Feed-Aktualisierungen auf ihren Desktops benötigen.

Deaktivieren der geplanten Datenträgerdefragmentierung auf übergeordneten virtuellen Windows 7-Maschinen

Bevor Sie verknüpfte Klone erstellen, müssen Sie die geplante Datenträgerdefragmentierung auf übergeordneten virtuellen Windows 7-Maschinen deaktivieren. Windows 7 plant standardmäßig eine wöchentliche Datenträgerdefragmentierung. Wiederholte Defragmentierungsvorgänge können die Linked-Clone-Betriebssystemfestplatten erheblich anwachsen lassen und verbessern den Festplattenzugriff auf verknüpfte Klone nur unwesentlich.

Wenn Sie einen Linked-Clone-Pool aus der übergeordneten virtuellen Maschine erstellen, nutzen die verknüpften Klone die Replikatfestplatte gemeinsam. Nachfolgende Defragmentierungsvorgänge wirken sich nicht auf die Replikatfestplatte aus, da diese schreibgeschützt ist. Stattdessen werden durch die Defragmentierung die Betriebssystemfestplatten der Klone vergrößert.

Als empfohlene Vorgehensweise sollten Sie die übergeordnete virtuelle Maschine einmalig defragmentieren, bevor Sie einen Snapshot erstellen und den Pool erstellen. Die verknüpften Klone profitieren von der Defragmentierung, da sie die optimierte schreibgeschützte Replikatfestplatte gemeinsam nutzen.

Voraussetzungen

- Stellen Sie sicher, dass die auf den verknüpften Klonen bereitzustellenden Anwendungen auf der virtuellen Maschine installiert sind.
- Vergewissern Sie sich, dass View Agent mit View Composer Agent auf der virtuellen Maschine installiert ist.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start]** und geben Sie im Feld **[Search programs and files (Programme/Dateien durchsuchen)]** den Befehl **`defrag`** ein.

4 Klicken Sie im Programmfenster auf **[Disk Defragmenter (Defragmentierung)]** .

5 Klicken Sie im Dialogfeld **[Disk Defragmenter (Defragmentierung)]** auf **[Defragment disk (Datenträger defragmentieren)]** .

Die Datenträgerdefragmentierung konsolidiert defragmentierte Dateien auf der Festplatte der virtuellen Maschine.

6 Klicken Sie im Dialogfeld **[Disk Defragmenter (Defragmentierung)]** auf **[Configure schedule (Zeitplan konfigurieren)]** .

7 Deaktivieren Sie die Option **[Run on a schedule (recommended) (Nach Zeitplan ausführen (empfohlen))]** und klicken Sie auf **[OK]** .

Es werden keine Defragmentierungsvorgänge auf virtuellen Linked-Clone-Maschinen durchgeführt, die über diese übergeordnete virtuelle Maschine erstellt werden.

Deaktivieren des Windows Update-Dienstes auf virtuellen Windows 7-Maschinen

Durch eine Deaktivierung des Windows Update-Dienstes können Sie die Anzahl der Dateierstellungen und der Schreibvorgänge verringern, die beim Herunterladen und Installieren von Updates auftreten. Auf diese Weise können Sie das Wachstum verknüpfter Klone und die Anzahl der E/A-Vorgänge pro Sekunde auf verknüpften Klonen und vollständigen virtuellen Maschinen verringern.

Deaktivieren Sie den Windows Update-Dienst, wenn Sie Linked-Clone-Desktops aktualisieren und neu zusammenstellen. Bei einer Aktualisierung werden die Betriebssystemfestplatten in den Zustand ihrer ursprünglichen Snapshots zurückversetzt und automatische Windows-Updates werden gelöscht. Bei einer Neuzusammenstellung werden die Betriebssystemfestplatten unter Verwendung eines neuen Snapshots erneut erstellt. Da dieser neue Snapshot die Windows-Updates möglicherweise bereits umfasst, sind automatische Windows-Updates überflüssig.

Deaktivieren Sie den Windows Update-Dienst nicht, wenn Sie Windows-Updates nicht über Neuzusammenstellungen auf den verknüpften Klonen installieren.

Voraussetzungen

Stellen Sie sicher, dass die neuesten Windows-Updates heruntergeladen und auf der virtuellen Maschine installiert wurden.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start] > [Control Panel (Systemsteuerung)] > [System and Security (System und Sicherheit)] > [Turn automatic updating on or off (Automatische Updates ein- oder ausschalten)]** .

4 Wählen Sie im Menü **[Important updates (Wichtige Updates)]** die Option **[Never check for updates (Nie auf Updates überprüfen)]** .

5 Deaktivieren Sie die Option **[Give me recommended updates the same way I receive important updates (Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen)]** .

6 Deaktivieren Sie die Option **[Allow all users to install updates on this computer (Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen)]** und klicken Sie auf **[OK]** .

Deaktivieren des Diagnoserichtliniendienstes auf virtuellen Windows 7-Maschinen

Durch das Deaktivieren des Windows-Diagnoserichtliniendienstes kann die Anzahl der Systemschreibvorgänge minimiert und das Wachstum von Linked-Clone-Desktops verringert werden.

Deaktivieren Sie den Windows-Diagnoserichtliniendienst nicht, wenn Ihre Benutzer die Diagnosetools auf ihren Desktops benötigen.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start] > [Control Panel (Systemsteuerung)] > [System and Security (System und Sicherheit)] > [Administrative Tools (Verwaltung)]** .

4 Wählen Sie **[Services (Dienste)]** und klicken Sie auf **[Open (Öffnen)]** .

5 Doppelklicken Sie auf **[Diagnostic Policy Service (Diagnoserichtliniendienst)]** .

6 Klicken Sie im Dialogfeld **[Diagnostic Policy Service Properties (Local Computer) (Eigenschaften von Diagnoserichtliniendienst (Lokaler Computer))]** auf **[Stop (Beenden)]** .

7 Wählen Sie im Menü **[Startup type (Starttyp)]** die Option **[Disabled (Deaktiviert)]** .

8 Klicken Sie auf **[OK]** .

Deaktivieren der Vorabruf- und SuperFetch-Funktionen auf virtuellen Windows 7-Maschinen

Durch das Deaktivieren der Vorabruf- und SuperFetch-Funktionen in Windows können Sie das Generieren von Vorabrufdateien und den Overhead vermeiden, der mit Vorabruf- und SuperFetch-Vorgängen verbunden ist. Auf diese Weise kann das Wachstum von Linked-Clone-Desktops verringert und die Anzahl der E/A-Vorgänge pro Sekunde auf vollständigen virtuellen Maschinen und verknüpften Klonen minimiert werden.

Zum Deaktivieren der Vorabruf- und SuperFetch-Funktionen müssen Sie einen Windows-Registrierungsschlüssel bearbeiten und den Vorabrufdienst auf der virtuellen Maschine deaktivieren.

Voraussetzungen

Informationen zur Verwendung des Windows-Registrierungs-Editors unter Windows 7 finden Sie auf der Microsoft TechNet-Website.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf der lokalen virtuellen Windows 7-Maschine.

2 Navigieren Sie zum Registrierungsschlüssel **[PrefetchParameters]** .

Der Registrierungsschlüssel befindet sich im folgenden Pfad: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`.

3 Legen Sie die Werte für **[EnablePrefetcher]** und **[EnableSuperfetch]** auf **0** fest.

4 Klicken Sie auf **[Start] > [Control Panel (Systemsteuerung)] > [System and Security (System und Sicherheit)] > [Administrative Tools (Verwaltung)]** .

5 Wählen Sie **[Services (Dienste)]** und klicken Sie auf **[Open (Öffnen)]** .

6 Doppelklicken Sie auf den Dienst **[Superfetch (SuperFetch)]** .

7 Klicken Sie im Dialogfeld **[Superfetch Properties (Local Computer) (Eigenschaften von SuperFetch (Lokaler Computer))]** auf **[Stop (Beenden)]** .

8 Wählen Sie im Menü **[Startup type (Starttyp)]** die Option **[Disabled (Deaktiviert)]** .

9 Klicken Sie auf **[OK]** .

Deaktivieren der Sicherung der Windows-Registrierung auf virtuellen Windows 7-Maschinen

Durch das Deaktivieren der Sicherung der Windows-Registrierung, `RegIdleBackup`, kann die Anzahl der Systemschreibvorgänge minimiert und das Wachstum von Linked-Clone-Desktops verringert werden.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start]** > **[Control Panel (Systemsteuerung)]** > **[System and Security (System und Sicherheit)]** > **[Administrative Tools (Verwaltung)]** .

4 Wählen Sie **[Task Scheduler (Aufgabenplanung)]** und klicken Sie auf **[Open (Öffnen)]** .

5 Erweitern Sie im linken Bereich **[Task Scheduler Library (Aufgabenplanungsbibliothek)]** , **[Microsoft]** , **[Windows]** .

6 Doppelklicken Sie auf **[Registry (Registrierung)]** und wählen Sie **[RegIdleBackup]** .

7 Klicken Sie im Fensterbereich **[Actions (Aktionen)]** auf **[Disable (Deaktivieren)]** .

Deaktivieren der Systemwiederherstellung auf virtuellen Windows 7-Maschinen

Sie benötigen die Windows-Funktion zur Systemwiederherstellung nicht, wenn Sie Linked-Clone-Betriebssystemfestplatten mithilfe der View Composer-Aktualisierung in den Zustand ihrer ursprünglichen Snapshots zurückversetzen.

Wenn sich das Betriebssystem im Leerlauf befindet, hat die Systemwiederherstellung keine sichtbare Auswirkung auf das Wachstum von Betriebssystemfestplatten. Wenn sich das Betriebssystem jedoch in Verwendung befindet, generiert die Systemwiederherstellung Wiederherstellungspunkte basierend auf der Systemverwendung. Dies kann erhebliche Auswirkungen auf das Wachstum von Betriebssystemfestplatten haben.

Die Funktion der Windows-Systemwiederherstellung entspricht der einer View Composer-Aktualisierung.

Als empfohlene Vorgehensweise können Sie die Windows-Systemwiederherstellung deaktivieren und ein unnötiges Wachstum Ihrer verknüpften Klone vermeiden.

Wenn Sie keine Aktualisierungen verwenden, wägen Sie ab, ob die Systemwiederherstellung in Ihrer View-Umgebung aktiviert bleiben sollte.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start]** > **[Control Panel (Systemsteuerung)]** > **[System and Security (System und Sicherheit)]** > **[Administrative Tools (Verwaltung)]** .

4 Wählen Sie **[Task Scheduler (Aufgabenplanung)]** und klicken Sie auf **[Open (Öffnen)]** .

5 Erweitern Sie im linken Bereich **[Task Scheduler Library (Aufgabenplanungsbibliothek)]** , **[Microsoft]** , **[Windows]** .

6 Doppelklicken Sie auf **[SystemRestore]** und wählen Sie **[SR]** .

7 Klicken Sie im Fensterbereich **[Actions (Aktionen)]** auf **[Disable (Deaktivieren)]** .

Deaktivieren von Windows Defender auf virtuellen Windows 7-Maschinen

Microsoft Windows Defender kann zu einem Wachstum von Linked-Clone-Betriebssystemfestplatten beitragen und die Anzahl an E/A-Vorgängen pro Sekunde auf verknüpften Klonen und vollständigen virtuellen Maschinen erhöhen. Deaktivieren Sie Windows Defender, wenn Sie eine andere Anti-Spyware-Software auf der virtuellen Maschine installiert haben.

Wenn Windows Defender die einzige installierte Anti-Spyware-Software auf der virtuellen Maschine ist, sollten Sie Windows Defender möglicherweise auf den Desktops in Ihrer Umgebung aktiviert lassen.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start]** und geben Sie im Feld **[Search programs and files (Programme/Dateien durchsuchen)]** den Befehl `Windows Defender` ein.

4 Klicken Sie auf **[Tools (Extras)] > [Options (Optionen)] > [Administrator]** .

5 Deaktivieren Sie die Option **[Use this program (Dieses Programm verwenden)]** und klicken Sie auf **[Save (Speichern)]** .

Deaktivieren der Microsoft-Feeds-Synchronisierung auf virtuellen Windows 7-Maschinen

Windows Internet Explorer 7 und 8 verwenden die Microsoft-Feeds-Synchronisierung, um RSS-Feeds in den Webbrowsern der Benutzer zu aktualisieren. Dieser Task kann zu einem Wachstum der verknüpften Klone beitragen. Deaktivieren Sie diesen Task, wenn Ihre Benutzer keine automatische Aktualisierung der RSS-Feeds in ihren Browsern benötigen.

Die Microsoft-Feeds-Synchronisierung kann zu einem Wachstum der Betriebssystemfestplatten führen, wenn keine persistenten Festplatten konfiguriert sind. Sind persistente Festplatten konfiguriert, gelten die Auswirkungen für die persistenten Festplatten. In dieser Situation sollten Sie dennoch die Microsoft-Feeds-Synchronisierung deaktivieren, um das Wachstum persistenter Festplatten zu kontrollieren.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows 7-Gastbetriebssystem als Administrator an.

3 Klicken Sie auf **[Start] > [Control Panel (Systemsteuerung)] > [Network and Internet (Netzwerk und Internet)] > [Internet Options (Internetoptionen)]** .

4 Klicken Sie auf die Registerkarte **[Content (Inhalt)]** .

5 Klicken Sie unter **[Feeds and Web Slices (Feeds und Web Slices)]** auf **[Settings (Einstellungen)]** .

6 Deaktivieren Sie die Option **[Automatically check feeds and Web Slices for updates (Feeds und Web Slices automatisch auf Aktualisierungen prüfen)]** und klicken Sie auf **[OK]** .

7 Klicken Sie im Dialogfeld **[Internet Properties (Interneteigenschaften)]** auf **[OK]** .

Vorbereiten virtueller Maschinen für View Composer

Sie müssen zum Bereitstellen von Linked-Clone-Desktops eine übergeordnete virtuelle Maschine vorbereiten, die die Anforderungen des View Composer-Dienstes erfüllt.

- Vorbereiten einer übergeordneten virtuellen Maschine auf Seite 75

  Für den View Composer-Dienst ist eine übergeordnete virtuelle Maschine erforderlich, mit der Sie ein Basis-Image zum Erstellen und Verwalten von Linked-Clone-Desktops generieren.

- Aktivieren von Windows 7 und Windows Vista auf Linked-Clone-Desktops auf Seite 77

  Um sicherzustellen, dass View Composer Windows 7- und Windows Vista-Betriebssysteme auf Linked-Clone-Desktops ordnungsgemäß aktiviert, müssen Sie die Microsoft-Volumenaktivierung auf der übergeordneten virtuellen Maschine verwenden. Für die Volumenaktivierungstechnologie ist ein Volumenlizenzschlüssel erforderlich.

- Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine auf Seite 78

  Die Option für den Windows-Ruhezustand erstellt eine umfangreiche Systemdatei, welche die Linked-Clone-Betriebssystemfestplatten vergrößern kann, die aus der übergeordneten virtuellen Maschine erstellt werden. Durch das Deaktivieren des Ruhezustands wird die Größe verknüpfter Klone verringert.

- Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers auf Seite 79

  Wenn Sie eine übergeordnete virtuelle Maschine für View Composer vorbereiten, können Sie die übergeordnete virtuelle Maschine sowie Linked-Clone-Desktops so konfigurieren, dass Auslagerungsdateien der virtuellen Maschine im lokalen Datenspeicher gespeichert werden. Bei dieser optionalen Strategie können Sie die Vorteile des lokalen Speichers nutzen.

- Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine auf Seite 79

  Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems an eine separate Festplatte umleiten. Sie müssen diese Festplatte so konfigurieren, dass sie größer ist als die Auslagerungsdatei im Gastbetriebssystem.

- Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts auf Seite 80

  View Composer beendet ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Sie können das Zeitüberschreitungslimit für diese Skripts erhöhen, indem Sie den Wert `ExecScriptTimeout` in der Windows-Registrierung auf der übergeordneten virtuellen Maschine ändern.

Vorbereiten einer übergeordneten virtuellen Maschine

Für den View Composer-Dienst ist eine übergeordnete virtuelle Maschine erforderlich, mit der Sie ein Basis-Image zum Erstellen und Verwalten von Linked-Clone-Desktops generieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie eine virtuelle Maschine zur Verwendung für bereitgestellte View-Desktops vorbereitet haben. Siehe „Erstellen virtueller Maschinen für die View-Desktop-Bereitstellung“, auf Seite 51.

Eine übergeordnete virtuelle Maschine, die Sie für View Composer verwenden, muss entweder zu derselben Active Directory-Domäne wie die Domäne gehören, mit der sich die Linked-Clone-Desktops verbinden, oder sie muss Mitglied der lokalen ARBEITSGRUPPE sein.

WICHTIG Um in View Manager 4.5 oder einer höheren Version unterstützte Funktionen wie z. B. das Umleiten löschbarer Dateien auf eine separate Festplatte und das Anpassen von Linked-Clone-Desktops mit Sysprep nutzen zu können, müssen Sie die Desktops anhand einer übergeordneten virtuelle Maschine bereitstellen, auf der View Agent 4.5 oder höher installiert ist.

Sie können View Composer nicht zur Bereitstellung von Desktops verwenden, auf denen die Windows Vista Ultimate Edition oder Windows XP Professional SP1 ausgeführt wird.

- Stellen Sie sicher, dass die virtuelle Maschine nicht von einem verknüpften Klon für View Composer konvertiert wurde. Eine virtuelle Maschine, die von einem verknüpften Klon konvertiert wurde, verfügt über die kloneigenen Informationen zu interner Festplatte und Status. Eine übergeordnete virtuelle Maschine kann nicht über Statusinformationen verfügen.
- Wenn auf der übergeordneten virtuellen Maschine Windows XP und Active Directory unter Windows Server 2008 ausgeführt wird, wenden Sie ein Update-Patch auf die virtuelle Windows XP-Maschine an. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 944043 unter der folgenden Adresse: http://support.microsoft.com/kb/944043/en-us.

  Wenn Sie das Windows Server 2008-RODC-Compatibility Pack für Windows XP nicht installieren, können über diese übergeordnete virtuelle Maschine bereitgestellte verknüpfte Klone nicht zur Domäne hinzugefügt werden.
- Wenn Sie View Agent auf der übergeordneten virtuellen Maschine installieren, wählen Sie die Option **[View Composer Agent]** aus. Siehe „Installieren von View Agent auf einer virtuellen Maschine“, auf Seite 57.

  Um View Agent in einer großen Umgebung zu aktualisieren, können Sie standardmäßige Windows-Aktualisierungsmethoden wie Altiris, SMS, LanDesk, BMC oder eine andere Software für die Systemverwaltung verwenden. Sie können zum Aktualisieren von View Agent auch den Vorgang der Neuzusammenstellung verwenden.

  HINWEIS Ändern Sie keinesfalls das Anmeldekonto für den VMware View Composer-Gastagentserver-Dienst in einer übergeordneten virtuellen Maschine. Standardmäßig handelt es sich hierbei um das lokale Systemkonto. Wenn Sie dieses Konto ändern, können die von der übergeordneten Maschine erstellten verknüpften Klone nicht gestartet werden.

- Zur Bereitstellung von Windows 7- oder Windows Vista-Desktops konfigurieren Sie einen Volumenlizenzschlüssel und aktivieren das Betriebssystem der übergeordneten virtuellen Maschine mit der Volumenaktivierung. Siehe „Aktivieren von Windows 7 und Windows Vista auf Linked-Clone-Desktops“, auf Seite 77.
- Wenn auf der übergeordneten virtuellen Maschine Windows 7 ausgeführt wird, müssen Sie sicherstellen, dass die empfohlenen Vorgehensweisen zur Optimierung des Betriebssystems ausgeführt wurden. Siehe „Optimieren von Windows 7 für Linked-Clone-Desktops“, auf Seite 66.

Vorgehensweise

- Entfernen Sie die DHCP-Lease auf der übergeordneten virtuellen Maschine, um das Kopieren einer geleasten IP-Adresse zu den verknüpften Klonen im Pool zu vermeiden.

  a Öffnen Sie auf der übergeordneten virtuellen Maschine eine Eingabeaufforderung.

  b Geben Sie den Befehl **`ipconfig /release`** ein.

- Stellen Sie sicher, dass die Systemfestplatte ein einzelnes Volume umfasst.

  Sie können keine verknüpften Klone von einer übergeordneten virtuellen Maschine bereitstellen, die mehr als ein Volume umfasst. Mit View Composer-Dienst werden mehrere Laufwerkpartitionen nicht unterstützt. Es werden mehrere virtuelle Festplatten unterstützt.

- Deaktivieren Sie die Option für den Ruhezustand, um die Größe der Linked-Clone-Betriebssystemfestplatten zu verringern, die aus der übergeordneten virtuellen Maschine erstellt werden.

- Deaktivieren Sie in vSphere Client die vApp-Optionseinstellung auf der übergeordneten virtuellen Maschine.

Sie können einen Linked-Clone-Pool von einer übergeordneten virtuellen Maschine bereitstellen.

Weiter

Verwenden Sie vSphere Client, um einen Snapshot der übergeordneten virtuellen Maschine im ausgeschalteten Zustand zu erstellen. Dieser Snapshot wird als Baselinekonfiguration für den ersten Satz an Linked-Clone-Desktops verwendet, die an die übergeordnete virtuelle Maschine gekoppelt sind.

WICHTIG Bevor Sie einen Snapshot erstellen, müssen Sie die übergeordnete virtuelle Maschine vollständig herunterfahren. Verwenden Sie hierzu den Befehl **[Shut Down (Herunterfahren)]** im Gastbetriebssystem.

Aktivieren von Windows 7 und Windows Vista auf Linked-Clone-Desktops

Um sicherzustellen, dass View Composer Windows 7- und Windows Vista-Betriebssysteme auf Linked-Clone-Desktops ordnungsgemäß aktiviert, müssen Sie die Microsoft-Volumenaktivierung auf der übergeordneten virtuellen Maschine verwenden. Für die Volumenaktivierungstechnologie ist ein Volumenlizenzschlüssel erforderlich.

Zur Aktivierung von Windows 7 oder Windows Vista mit Volumenaktivierung müssen Sie den Schlüsselverwaltungsdienst (Key Management Service, KMS) verwenden, für den ein KMS-Lizenzschlüssel erforderlich ist. Wenden Sie sich an Ihren Microsoft-Händler, um einen Volumenlizenzschlüssel zu erhalten und die Volumenaktivierung zu konfigurieren.

HINWEIS View Composer bietet keine Unterstützung für die MAK-Lizenzierung (Multiple Activation Key).

Bevor Sie mit View Composer Linked-Clone-Desktops erstellen können, müssen Sie die Volumenaktivierung verwenden, um das Betriebssystem auf der übergeordneten virtuellen Maschine zu aktivieren.

HINWEIS Bei Windows XP-Desktops mit Volumenlizenzen ist keine Aktivierung notwendig.

Bei der Erstellung eines Linked-Clone-Desktops und bei jeder Neuzusammenstellung des verknüpften Klons verwendet View Composer Agent den KMS-Server der übergeordneten virtuellen Maschine, um das Betriebssystem auf dem verknüpften Klon zu aktivieren.

Das View Composer QuickPrep-Tool führt zur Aktivierung die folgenden Schritte aus:

1 Aufruf eines Skripts, um den aktuellen Lizenzstatus auf der virtuellen Linked-Clone-Maschine zu entfernen

2 Neustart des Gastbetriebssystems

3 Aufruf eines Skripts, das mithilfe der KMS-Lizenzierung das Betriebssystem auf dem Klon aktiviert.

Die Aktivierung wird bei jeder Ausführung von QuickPrep auf einem verknüpften Klon durchgeführt.

View Composer verwendet für die KMS-Lizenzierung den KMS-Server, der für die Aktivierung der übergeordneten virtuellen Maschine konfiguriert ist. Der KMS-Server behandelt einen aktivierten verknüpften Klon als einen Computer mit einer neu ausgegebenen Lizenz.

Deaktivieren des Windows-Ruhezustands in der übergeordneten virtuellen Maschine

Die Option für den Windows-Ruhezustand erstellt eine umfangreiche Systemdatei, welche die Linked-Clone-Betriebssystemfestplatten vergrößern kann, die aus der übergeordneten virtuellen Maschine erstellt werden. Durch das Deaktivieren des Ruhezustands wird die Größe verknüpfter Klone verringert.

Die Option für den Windows-Ruhezustand erstellt eine versteckte Systemdatei, `Hiberfil.sys`. Windows verwendet diese Datei, um eine Kopie des Systemarbeitsspeichers auf der Festplatte zu speichern, wenn die Funktion für den hybriden Standbymodus aktiviert ist. Wenn Sie einen Linked-Clone-Pool erstellen, wird die Datei auf der Betriebssystemfestplatte für jeden verknüpften Klon erstellt.

Auf virtuellen Windows 7-Maschinen kann diese Datei bis zu 10 GB groß sein.

Vorsicht Wenn Sie den Ruhezustand deaktivieren, funktioniert die Einstellung für den hybriden Standbymodus nicht. Benutzer können Daten verlieren, wenn die Einstellung für den hybriden Standbymodus eingeschaltet ist und es zu einem Stromausfall kommt.

Voraussetzungen

Machen Sie sich mit der Funktion für den Windows-Ruhezustand vertraut. Informationen finden Sie auf der Website des Microsoft-Supports. Informationen zum Deaktivieren des Ruhezustands unter Windows 7 oder Windows Vista finden Sie ebenfalls auf der Website des Microsoft-Supports. Suchen Sie nach der Vorgehensweise für das Deaktivieren und erneute Aktivieren des Ruhezustands auf einem Computer, auf dem Windows ausgeführt wird.

Vorgehensweise

1 Markieren Sie in vSphere Client die übergeordnete virtuelle Maschine und wählen Sie **[Open Console (Konsole öffnen)]** .

2 Melden Sie sich am Windows-Gastbetriebssystem als Administrator an.

3 Deaktivieren Sie die Option für den Ruhezustand.

Betriebssystem	Aktion
Windows 7 oder Windows Vista	a Klicken Sie auf **[Start]** und geben Sie im Feld **[Start Search (Suche starten)]** den Befehl **`cmd`** ein. b Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf **[Command Prompt (Eingabeaufforderung)]** und klicken Sie auf **[Run as Administrator (Als Administrator ausführen)]** . c Klicken Sie an der Eingabeaufforderung der Benutzerkontensteuerung auf **[Continue (Weiter)]** . d Geben Sie an der Eingabeaufforderung **`powercfg.exe /hibernate off`** ein und drücken Sie die Eingabetaste. e Geben Sie **`exit`** ein und drücken Sie die Eingabetaste.
Windows XP	a Klicken Sie auf **[Start] > [Run (Ausführen)]** . b Geben Sie **`cmd`** ein und klicken Sie auf **[OK]** . c Geben Sie an der Eingabeaufforderung **`powercfg.exe /hibernate off`** ein und drücken Sie die Eingabetaste. d Geben Sie **`exit`** ein und drücken Sie die Eingabetaste.

4 Melden Sie sich vom Gastbetriebssystem ab.

Wenn Sie Linked-Clone-Desktops aus der übergeordneten virtuellen Maschine erstellt haben, wird die Datei `Hiberfil.sys` nicht auf den Linked-Clone-Betriebssystemfestplatten erstellt.

Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers

Wenn Sie eine übergeordnete virtuelle Maschine für View Composer vorbereiten, können Sie die übergeordnete virtuelle Maschine sowie Linked-Clone-Desktops so konfigurieren, dass Auslagerungsdateien der virtuellen Maschine im lokalen Datenspeicher gespeichert werden. Bei dieser optionalen Strategie können Sie die Vorteile des lokalen Speichers nutzen.

Bei dieser Vorgehensweise können Sie den lokalen Speicher für die Auslagerungsdateien der virtuellen Maschine und nicht die Auslagerungsdateien und temporären Dateien im Gastbetriebssystem konfigurieren. Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems zu einer separaten Festplatte umleiten. Siehe „Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools“, auf Seite 89.

Voraussetzungen

Bereiten Sie die übergeordnete virtuelle Maschine vor, damit die Anforderungen des View Composer-Dienstes erfüllt werden. Siehe „Vorbereiten einer übergeordneten virtuellen Maschine“, auf Seite 75.

Vorgehensweise

1 Konfigurieren Sie einen Auslagerungsdatei-Datenspeicher auf dem ESX/ESXi-Host oder -Cluster, auf dem Sie den Linked-Clone-Pool bereitstellen möchten.

2 Wenn Sie die übergeordnete virtuelle Maschine in vCenter Server erstellen, speichern Sie die Auslagerungsdateien der virtuellen Maschine im Auslagerungsdatei-Datenspeicher auf dem lokalen ESX/ESXi-Host oder -Cluster:

   a Wählen Sie in vSphere Client die übergeordnete virtuelle Maschine aus.

   b Klicken Sie auf **[Edit Settings (Einstellungen bearbeiten)]** und anschließend auf die Registerkarte **[Options (Optionen)]** .

   c Klicken Sie auf **[Swapfile location (Speicherort der Auslagerungsdatei)]** und auf **[Store in the host's swapfile datastore (Im Auslagerungsdatei-Datenspeicher des Hosts speichern)]** .

   Weitere Anweisungen finden Sie in der VMware vSphere-Dokumentation.

Wenn Sie einen Pool aus dieser übergeordneten virtuellen Maschine bereitstellen, verwenden die Linked-Clone-Desktops den Auslagerungsdatei-Datenspeicher des lokalen ESX-Hosts.

Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine

Wenn Sie einen Linked-Clone-Pool erstellen, können Sie Auslagerungsdateien und temporäre Dateien des Gastbetriebssystems an eine separate Festplatte umleiten. Sie müssen diese Festplatte so konfigurieren, dass sie größer ist als die Auslagerungsdatei im Gastbetriebssystem.

Wenn ein verknüpfter Klon, der mit einer separaten Festplatte für die löschbaren Dateien konfiguriert ist, ausgeschaltet wird, ersetzt View Manager die temporäre Festplatte mit einer Kopie der ursprünglichen temporären Festplatte, die View Composer mit dem Linked-Clone-Pool erstellt hat. Diese Funktion kann das Wachstum verknüpfter Klone verlangsamen. Diese Funktion kann jedoch nur verwendet werden, wenn die Größe der Festplatte mit löschbaren Dateien ausreicht, um die Auslagerungsdateien des Gastbetriebssystems aufzunehmen.

Bevor Sie die Festplatte für löschbare Dateien konfigurieren können, müssen Sie die maximale Auslagerungsdateigröße in der übergeordneten virtuellen Maschine kennen. Die Auslagerungsdatei der verknüpften Klone weist dieselbe Größe auf wie die Auslagerungsdatei der übergeordneten virtuellen Maschine, aus der die verknüpften Klone erstellt wurden.

HINWEIS Diese Funktion ist nicht mit der Konfiguration von lokalem Speicher für die Auslagerungsdateien der virtuellen Maschine identisch. Siehe „Konfigurieren einer übergeordneten virtuellen Maschine zur Verwendung des lokalen Speichers“, auf Seite 79.

Vorgehensweise

1 Klicken Sie in vSphere Client mit der rechten Maustaste auf die übergeordnete virtuelle Maschine und klicken Sie dann auf **[Open Console (Konsole öffnen)]** .

2 Wählen Sie **[Start]** > **[Settings (Einstellungen)]** > **[Control Panel (Systemsteuerung)]** > **[System]** .

3 Klicken Sie auf die Registerkarte **[Advanced (Erweitert)]** .

4 Klicken Sie im Fensterbereich **[Performance (Leistung)]** auf **[Settings (Einstellungen)]** .

5 Klicken Sie auf die Registerkarte **[Advanced (Erweitert)]** .

6 Klicken Sie im Fensterbereich **[Virtual memory (Virtueller Arbeitsspeicher)]** auf **[Change (Ändern)]** .

Die Seite **[Virtual memory (Virtueller Arbeitsspeicher)]** wird angezeigt.

7 Legen Sie für die Auslagerungsdateigröße einen höheren Wert fest als für den Arbeitsspeicher, der der virtuellen Maschine zugewiesen ist.

WICHTIG Wenn die Einstellung **[Maximum size (MB) (Maximale Größe (MB))]** kleiner ist als die Arbeitsspeichergröße der virtuellen Maschine, geben Sie einen höheren Wert ein und speichern Sie den neuen Wert.

8 Notieren Sie sich die Einstellung **[Maximum size (MB) (Maximale Größe (MB))]** , die im Fensterbereich Paging file size for selected drive (Auslagerungsdateigröße für ausgewähltes Laufwerk) konfiguriert ist.

Weiter

Wenn Sie einen Linked-Clone-Pool über diese übergeordnete virtuelle Maschine konfigurieren, konfigurieren Sie eine Festplatte für löschbare Dateien, die größer ist als die Auslagerungsdateigröße.

Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts

View Composer beendet ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Sie können das Zeitüberschreitungslimit für diese Skripts erhöhen, indem Sie den Wert `ExecScriptTimeout` in der Windows-Registrierung auf der übergeordneten virtuellen Maschine ändern.

Das höhere Zeitüberschreitungslimit wird auf verknüpfte Klone übertragen, die aus der übergeordneten virtuellen Maschine erstellt werden. QuickPrep-Anpassungsskripte können auf den verknüpften Klonen für die von Ihnen angegebene Zeit ausgeführt werden.

Alternativ dazu können Sie mit Ihrem Anpassungsskript ein weiteres Skript oder einen Prozess starten, durch das bzw. den die Aufgabe mit langer Laufzeit durchgeführt wird.

HINWEIS Die meisten QuickPrep-Anpassungsskripts werden innerhalb des Limits von 20 Sekunden ausgeführt. Testen Sie Ihre Skripts, bevor Sie das Limit erhöhen.

Voraussetzungen

- Installieren Sie View Agent mit der Option **[View Composer Agent]** auf der übergeordneten virtuellen Maschine.

- Stellen Sie sicher, dass die übergeordnete virtuelle Maschine für die Erstellung eines Linked-Clone-Pools vorbereitet ist. Siehe „Vorbereiten einer übergeordneten virtuellen Maschine“, auf Seite 75.

Vorgehensweise

1 Starten Sie auf der übergeordneten virtuellen Maschine den Windows-Registrierungs-Editor.

   a Wählen Sie **[Start]** > **[Command Prompt (Eingabeaufforderung)]** .

   b Geben Sie an der Eingabeaufforderung den Befehl **[regedit]** ein.

2 Suchen Sie in der Windows-Registrierung den Registrierungsschlüssel `vmware-viewcomposer-ga`.

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
   ```

3 Klicken Sie auf **[Edit (Bearbeiten)]** und bearbeiten Sie den Wert in der Registrierung.

   ```
   Value Name (Name): ExecScriptTimeout
   Value Type (Typ): REG_DWORD
   Value unit (Einheit): milliseconds
   ```

   Der Standardwert lautet 20000 Millisekunden.

Der Zeitüberschreitungswert wird erhöht. Sie müssen Windows nicht neu starten, damit dieser Wert wirksam wird.

Weiter

Erstellen Sie einen Snapshot der übergeordneten virtuellen Maschine sowie einen Linked-Clone-Pool.

Erstellen von Vorlagen virtueller Maschinen

Sie müssen eine Vorlage virtueller Maschinen erstellen, bevor Sie einen automatisierten Pool mit vollständigen virtuellen Maschinen erstellen können.

Eine Vorlage einer virtuellen Maschine ist eine Masterkopie einer virtuellen Maschine, die zum Erstellen und Bereitstellen neuer virtueller Maschinen verwendet werden kann. Eine Vorlage umfasst im Allgemeinen ein installiertes Gastbetriebssystem und einen Satz an Anwendungen.

Sie erstellen Vorlagen virtueller Maschinen in vSphere Client. Sie können eine Vorlage einer virtuellen Maschine von einer zuvor konfigurierten virtuellen Maschine erstellen oder eine zuvor konfigurierte virtuelle Maschine zu einer Vorlage einer virtuellen Maschine umwandeln.

Weitere Informationen zum Verwenden von vSphere Client, um Vorlagen virtueller Maschinen zu erstellen, finden Sie im Handbuch *vSphere Basic System Administration*. Weitere Informationen zum Erstellen von automatisierten Pools finden Sie unter „Automatisierte Pools mit vollständigen virtuellen Maschinen“, auf Seite 84.

Hinweis Anhand einer Vorlage für eine virtuelle Maschine erstellen Sie keinen Linked-Clone-Pool.

Erstellen von Anpassungsspezifikationen

Anpassungsspezifikationen sind optional, können jedoch die Bereitstellung von automatisierten Desktop-Pools erheblich beschleunigen. Möglich wird dies durch die Vorgabe von Konfigurationsinformationen für allgemeine Eigenschaften, beispielsweise Lizenzierung, Domänenanbindung und DHCP-Einstellungen.

Sie können mit Anpassungsspezifikationen View-Desktops anpassen, wenn sie in View Administrator erstellt werden. Sie können mit dem Assistenten für Anpassungsspezifikationen in vSphere Client neue Anpassungsspezifikationen erstellen. Sie können den Assistenten für Anpassungsspezifikationen auch verwenden, um die vorhandene benutzerdefinierte Datei `sysprep.ini` zu importieren.

Informationen zur Verwendung des Assistenten für Anpassungsspezifikationen finden Sie im Dokument *Verwaltung virtueller vSphere-Maschinen*.

Stellen Sie die Richtigkeit der Anpassungsspezifikationen sicher, bevor Sie sie in View Administrator verwenden. In vSphere Client führen Sie die Bereitstellung und Anpassung einer virtuellen Maschine anhand Ihrer Vorlage mithilfe von Anpassungsspezifikationen durch. Führen Sie vollständige Tests der virtuellen Maschine durch (einschließlich DHCP und Authentifizierung), bevor Sie View-Desktops erstellen.

HINWEIS Um Anpassungsspezifikationen auf Desktop-Pools anzuwenden, die Windows XP verwenden, müssen Sie die Microsoft Sysprep-Tools auf Ihrer vCenter Server-Maschine installieren.

Sie müssen keine Sysprep-Tools in vCenter Server für Desktop-Pools installieren, die Windows 7 oder Vista verwenden. Sysprep-Tools sind in diesen Betriebssystemen integriert.

Wenn Sie eine Sysprep-Anpassungsspezifikation verwenden, um einen Windows 7-Desktop zu einer Domäne hinzuzufügen, müssen Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der Active Directory-Domäne verwenden. Es ist nicht möglich, den NetBIOS-Namen der Active Directory-Domäne zu verwenden.

Erstellen von Desktop-Pools 5

Mit View Manager erstellen Sie Desktop-Pools, die Clients Zugriff auf View-Desktops bieten. View Manager stellt Pools aus Desktop-Quellen bereit. Hierbei kann es sich um virtuelle Maschinen, die von vCenter Server verwaltet werden, um virtuelle Maschinen, die auf einer anderen Virtualisierungsplattform ausgeführt werden, oder um physische Computer, Terminalserver oder Blade-PCs handeln.

Sie können mehrere Arten von Desktop-Pools erstellen. Außerdem können Sie einen einzelnen Desktop bereitstellen, indem Sie einen manuellen Pool mit einer einzigen Desktop-Quelle bereitstellen.

- Automatisierte Pools mit vollständigen virtuellen Maschinen auf Seite 84

  Zur Erstellung eines automatisierten Desktop-Pools stellt View Manager Desktops dynamisch basierend auf Einstellungen bereit, die Sie auf den Pool anwenden. View Manager verwendet eine Vorlage für virtuelle Maschinen als Desktop-Quelle für den Pool und erstellt für jeden Desktop eine neue virtuelle Maschine in vCenter Server.

- Pools von Linked-Clone-Desktops auf Seite 89

  Zum Erstellen eines Pools von Linked-Clone-Desktops generiert View Composer virtuelle Linked-Clone-Maschinen aus einem Snapshot einer übergeordneten virtuellen Maschine. View Manager stellt die Linked-Clone-Desktops dynamisch basierend auf den Einstellungen bereit, die Sie auf den Pool anwenden.

- Manuelle Desktop-Pools auf Seite 111

  Zum Erstellen eines manuellen Desktop-Pools stellt View Manager Desktops von vorhandenen Desktop-Quellen bereit. Für jeden Desktop im Pool wählen Sie eine separate Desktop-Quelle bereit, um den Clients View-Zugriff zu ermöglichen.

- Microsoft-Terminaldienste-Pools auf Seite 116

  Sie können Microsoft-Terminalserver einsetzen, um Terminaldienste-Sitzungen als Desktops für View-Clients bereitzustellen. View Manager verwaltet Terminaldienste-Sitzungen auf dieselbe Weise wie andere View-Desktops.

- Bereitstellen von Desktop-Pools auf Seite 118

  Bei der Erstellung eines Desktop-Pools legen Sie mithilfe von Konfigurationsoptionen fest, wie der Pool verwaltet wird und wie Benutzer mit den Desktops interagieren.

- Einstellen von Betriebsrichtlinien für Desktop-Pools auf Seite 132

  Sie können eine Betriebsrichtlinie für die virtuellen Maschinen in einem Desktop-Pool konfigurieren, wenn die virtuellen Maschinen über vCenter Server verwaltet werden.

Automatisierte Pools mit vollständigen virtuellen Maschinen

Zur Erstellung eines automatisierten Desktop-Pools stellt View Manager Desktops dynamisch basierend auf Einstellungen bereit, die Sie auf den Pool anwenden. View Manager verwendet eine Vorlage für virtuelle Maschinen als Desktop-Quelle für den Pool und erstellt für jeden Desktop eine neue virtuelle Maschine in vCenter Server.

Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen

Bei der Erstellung eines automatisierten Desktop-Pools fordert der View Administrator-Assistent Add Pool (Hinzufügen von Pools) Sie zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten Add Pool (Hinzufügen von Pools) angeben möchten.

Informationen zum Erstellen eines Linked-Clone-Pools finden Sie unter „Pools von Linked-Clone-Desktops“, auf Seite 89.

Tabelle 5-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen

Option	Beschreibung	Wert
User assignment (Benutzerzuweisung)	Wählen Sie die Art der Benutzerzuweisung: ■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Desktop zugewiesen. Benutzer erhalten bei jeder Anmeldung denselben Desktop. ■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Desktop. Weitere Informationen finden Sie unter „Benutzerzuweisung in Desktop-Pools“, auf Seite 119.	
Enable automatic assignment (Automatische Zuweisung aktivieren)	In einem Pool mit dedizierter Zuweisung wird ein Desktop einem Benutzer zugewiesen, wenn der Benutzer sich erstmals am Pool anmeldet. Sie können den Benutzern ihre Desktops auch explizit zuweisen. Wenn Sie die automatische Zuweisung nicht aktivieren, müssen Sie jedem Benutzer explizit einen Desktop zuweisen.	
vCenter Server	Wählen Sie die vCenter Server-Instanz aus, welche die virtuellen Maschinen im Pool verwaltet.	
Pool ID (Pool-ID)	Der eindeutige Name, der den Pool in View Administrator identifiziert. Wenn mehrere vCenter Server-Instanzen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere vCenter Server-Instanz dieselbe Pool-ID verwendet. Eine View Connection Server-Konfiguration kann eine eigenständige View Connection Server-Instanz oder eine Gruppe replizierter Instanzen sein, die eine gemeinsame View LDAP-Konfiguration nutzen.	

Tabelle 5-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen (Fortsetzung)

Option	Beschreibung	Wert
Display name (Anzeigename)	Der Pool-Name, der Benutzern bei ihrer Anmeldung an View Client angezeigt wird. Wenn Sie keinen Anzeigenamen angeben, wird den Benutzern die Pool-ID angezeigt.	
View Folder (View-Ordner)	Wählen Sie einen View-Ordner aus, in dem der Pool abgelegt wird, oder belassen Sie den Pool im Standard-Stammordner. Wenn Sie einen View-Ordner verwenden, können Sie die Verwaltung von Pools an einen Administrator mit einer bestimmten Rolle delegieren. Weitere Informationen finden Sie unter „Verwenden von Ordnern für die Verwaltungsdelegierung“, auf Seite 28. **Hinweis** View-Ordner unterscheiden sich von vCenter Server-Ordnern, in denen virtuelle Desktop-Maschinen gespeichert werden. Sie wählen einen vCenter Server-Ordner zusammen mit anderen vCenter Server-Einstellungen an einer späteren Stelle im Assistenten aus.	
Delete desktop after logoff (Desktop nach Abmeldung löschen)	Wenn Sie die dynamische Benutzerzuweisung auswählen, legen Sie fest, ob Desktops nach der Benutzerabmeldung gelöscht werden. **Hinweis** Diese Option wird auf der Seite mit den Pool-Einstellungen festgelegt.	
Pool Settings (Pool-Einstellungen)	Einstellungen, die den Desktop-Status, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen. Eine Beschreibung finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126. Eine Liste der Einstellungen für automatisierte Pools finden Sie unter „Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen“, auf Seite 88. Weitere Informationen über Betriebsrichtlinien und automatisierte Pools finden Sie unter „Einstellen von Betriebsrichtlinien für Desktop-Pools“, auf Seite 132.	
Virtual machine naming (Benennung virtueller Maschinen)	Wählen Sie, ob Desktops durch die manuelle Angabe einer Liste mit Desktop-Namen oder durch Bereitstellung eines Benennungsmusters sowie der Gesamtzahl an Desktops bereitgestellt werden sollen. Weitere Informationen finden Sie unter „Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters“, auf Seite 119.	
List of desktop names (Liste mit Desktop-Namen)	Wenn Sie Namen manuell angeben, bereiten Sie eine Textdatei vor, in der die Desktop-Namen aufgeführt sind. Optional können Sie auch die verknüpften Benutzernamen angeben.	

Tabelle 5-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen (Fortsetzung)

Option	Beschreibung	Wert
Naming pattern (Benennungsmuster)	Wenn Sie diese Benennungsmethode verwenden, stellen Sie das Muster bereit. View Manager verwendet Ihr Muster als Präfix in allen Desktop-Namen und hängt eine eindeutige Zahl zur Identifizierung der einzelnen Desktops an. Weitere Informationen finden Sie unter „Verwenden eines Benennungsmusters für automatisierte Desktop-Pools“, auf Seite 122.	
Maximum number of desktops (Maximale Anzahl an Desktops)	Wenn Sie ein Benennungsmuster verwenden, geben Sie die Gesamtzahl an Desktops im Pool an. Außerdem können Sie bei der ersten Erstellung des Pools eine Mindestzahl an bereitzustellenden Desktops angeben.	
Number of spare (powered on) desktops (Anzahl an eingeschalteten Reserve-Desktops)	Wenn Sie Namen manuell angeben oder ein Benennungsmuster verwenden, geben Sie eine Anzahl an Desktops an, die View Manager für neue Benutzer verfügbar und eingeschaltet hält. Weitere Informationen finden Sie unter „Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters“, auf Seite 119. Wenn Sie Namen manuell festlegen, heißt diese Option **[# Unassigned desktops kept powered on (Anzahl an ständig eingeschalteten nicht zugewiesenen Desktops)]** .	
Minimum number of desktops (Mindestanzahl an Desktops)	Wenn Sie ein Benennungsmuster verwenden und Desktops nach Bedarf bereitstellen, geben Sie eine Mindestanzahl an Desktops im Pool an. Wenn Sie Desktops nach Bedarf bereitstellen, erstellt View Manager Desktops, sobald Benutzer sich erstmals am Pool anmelden. View Manager erstellt die Mindestanzahl an Desktops bei der Erstellung des Pools.	
Template (Vorlage)	Wählen Sie die Vorlage für virtuelle Maschinen aus, die View Manager zum Erstellen des Pools verwendet.	
vCenter Server folder (vCenter Server-Ordner)	Wählen Sie den Ordner in vCenter Server aus, in dem der Desktop-Pool gespeichert wird.	
Host or cluster (Host oder Cluster)	Wählen Sie den ESX-Host oder -Cluster aus, in dem die virtuellen Desktop-Maschinen ausgeführt werden.	
Resource pool (Ressourcen-Pool)	Wählen Sie den vCenter Server-Ressourcen-Pool aus, in dem der Desktop-Pool gespeichert ist.	

Tabelle 5-1. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen (Fortsetzung)

Option	Beschreibung	Wert
Datastores (Datenspeicher)	Wählen Sie einen oder mehrere Datenspeicher zur Speicherung des Desktop-Pools aus. Für Cluster können Sie freigegebene oder lokal gespeicherte Datenspeicher verwenden.	
Guest customization (Gastanpassung)	Wählen Sie eine Anpassungsspezifikation (SYSPREP) aus der Liste aus, damit View Manager die Lizenzierung, die Domänenbindung, DHCP-Einstellungen und andere Eigenschaften auf den Desktops konfiguriert. Alternativ dazu können Sie die Desktops nach der Erstellung durch View Manager manuell anpassen.	

Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen

Sie können einen automatisierten Desktop-Pool basierend auf einer von Ihnen ausgewählten Vorlage für virtuelle Maschinen erstellen. View Manager stellt die Desktops dynamisch bereit und erstellt dabei für jeden Desktop eine neue virtuelle Maschine in vCenter Server.

Informationen zum Erstellen eines Linked-Clone-Pools finden Sie unter „Pools von Linked-Clone-Desktops“, auf Seite 89.

Voraussetzungen

- Bereiten Sie eine Vorlage für virtuelle Maschinen vor, die View Manager zum Erstellen der Desktops verwendet. View Agent muss in der Vorlage installiert sein. Siehe Kapitel 4, „Erstellen und Vorbereiten virtueller Maschinen“, auf Seite 51.
- Wenn Sie eine Anpassungsspezifikation verwenden möchten, müssen Sie die Richtigkeit der Spezifikationen sicherstellen. In vSphere Client führen Sie die Bereitstellung und Anpassung einer virtuellen Maschine anhand Ihrer Vorlage mithilfe von Anpassungsspezifikationen durch. Führen Sie vollständige Tests der virtuellen Maschine durch, einschließlich DHCP und Authentifizierung.
- Stellen Sie sicher, dass Sie auf dem virtuellen ESX-Switch, der für virtuelle Desktop-Maschinen verwendet wird, über eine ausreichende Anzahl an Ports verfügen. Der Standardwert reicht möglicherweise nicht aus, wenn Sie große Desktop-Pools erstellen. Die Anzahl der Ports für den virtuellen Switch auf dem ESX-Host muss der Anzahl der virtuellen Desktop-Maschinen multipliziert mit der Anzahl der virtuellen Netzwerkkarten pro virtueller Maschine entsprechen (oder diese übersteigen).
- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe „Arbeitsblatt zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen“, auf Seite 84.
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe „Desktop- und Pool-Einstellungen“, auf Seite 126.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Klicken Sie auf **[Add (Hinzufügen)]** .

3 Wählen Sie **[Automated Pool (Automatisierter Pool)]** aus.

4 Wählen Sie auf der Seite vCenter Server die Option **[Full virtual machines (Vollständige virtuelle Maschinen)]** .

5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

In View Administrator können Sie die Desktops so anzeigen, wie sie dem Pool hinzugefügt werden. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Desktops]** .

Weiter

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139.

Desktop-Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen

Bei der Konfiguration automatisierter Pools mit vollständigen virtuellen Maschinen müssen Sie Desktop- und Pool-Einstellungen angeben. Für Pools mit dedizierten Benutzerzuweisungen und dynamischen Benutzerzuweisungen gelten unterschiedliche Einstellungen.

Tabelle 5-2 werden die Einstellungen aufgeführt, die für automatisierte Pools mit dedizierten Zuweisungen und dynamischen Zuweisungen gelten.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126.

Tabelle 5-2. Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen

Einstellung	Automatisierter Pool, dedizierte Zuweisung	Automatisierter Pool, dynamische Zuweisung
State (Status)	Ja	Ja
Connection Server Restrictions (Einschränkungen für Connection Server)	Ja	Ja
Betriebsrichtlinie für Remote-Desktops	Ja	Ja
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	Ja	Ja
Allow users to reset their desktops (Benutzern das Zurücksetzen ihrer Desktops gestatten)	Ja	Ja
Allow multiple sessions per user (Mehrere Sitzungen pro Benutzer zulassen)		Ja
Delete desktop after logoff (Desktop nach Abmeldung löschen)		Ja
Default display protocol (Standardanzeigeprotokoll)	Ja	Ja
Allow users to choose a protocol (Benutzern die Wahl des Protokolls erlauben)	Ja	Ja
Windows 7-3D-Rendering	Ja	Ja
Max number of monitors (Maximale Anzahl an Monitoren)	Ja	Ja
Max resolution of any one monitor (Max. Auflösung eines Monitors)	Ja	Ja

Tabelle 5-2. Einstellungen für automatisierte Pools mit vollständigen virtuellen Maschinen (Fortsetzung)

Einstellung	Automatisierter Pool, dedizierte Zuweisung	Automatisierter Pool, dynamische Zuweisung
Adobe Flash quality (Adobe Flash-Qualität)	Ja	Ja
Adobe Flash throttling (Adobe Flash-Drosselung)	Ja	Ja

Pools von Linked-Clone-Desktops

Zum Erstellen eines Pools von Linked-Clone-Desktops generiert View Composer virtuelle Linked-Clone-Maschinen aus einem Snapshot einer übergeordneten virtuellen Maschine. View Manager stellt die Linked-Clone-Desktops dynamisch basierend auf den Einstellungen bereit, die Sie auf den Pool anwenden.

Da Linked-Clone-Desktops ein Basis-Image der Systemfestplatte gemeinsam nutzen, benötigen sie weniger Speicher als vollständige virtuelle Maschinen.

Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools

Bei der Erstellung eines Linked-Clone-Desktop-Pools fordert Sie der View Administrator-Assistent Add Pool (Hinzufügen von Pools) zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten Add Pool (Hinzufügen von Pools) angeben möchten.

Bevor Sie einen Linked-Clone-Pool erstellen, müssen Sie mithilfe von vCenter Server einen Snapshot der übergeordneten virtuellen Maschine erstellen, die Sie für den Pool vorbereiten. Vor dem Erstellen des Snapshots müssen Sie die übergeordnete virtuelle Maschine herunterfahren. View Composer verwendet den Snapshot als Basis-Image, von dem die Klone erstellt werden.

Hinweis Sie können aus einer Vorlage für virtuelle Maschinen keinen Linked-Clone-Pool erstellen.

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools

Option	Beschreibung	Wert
User assignment (Benutzerzuweisung)	Wählen Sie die Art der Benutzerzuweisung: ■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Desktop zugewiesen. Benutzer erhalten bei jeder Anmeldung denselben Desktop. ■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Desktop. Weitere Informationen finden Sie unter „Benutzerzuweisung in Desktop-Pools“, auf Seite 119.	
Enable automatic assignment (Automatische Zuweisung aktivieren)	In einem Pool mit dedizierter Zuweisung wird ein Desktop einem Benutzer zugewiesen, wenn der Benutzer sich erstmals am Pool anmeldet. Sie können den Benutzern ihre Desktops auch explizit zuweisen. Wenn Sie die automatische Zuweisung nicht aktivieren, müssen Sie jedem Benutzer explizit einen Desktop zuweisen.	
vCenter Server	Wählen Sie die vCenter Server-Instanz aus, welche die virtuellen Maschinen im Pool verwaltet.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Pool ID (Pool-ID)	Der eindeutige Name, der den Pool in View Administrator identifiziert. Wenn mehrere View Connection Server-Konfigurationen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere View Connection Server-Konfiguration dieselbe Pool-ID verwendet. Eine View Connection Server-Konfiguration kann eine eigenständige View Connection Server-Instanz oder eine Gruppe replizierter Instanzen sein, die eine gemeinsame View LDAP-Konfiguration nutzen.	
Display name (Anzeigename)	Der Pool-Name, der Benutzern bei ihrer Anmeldung an View Client angezeigt wird. Wenn Sie keinen Anzeigenamen angeben, wird den Benutzern die Pool-ID angezeigt.	
View Folder (View-Ordner)	Wählen Sie einen View-Ordner aus, in dem der Pool abgelegt wird, oder belassen Sie den Pool im Standard-Stammordner. Wenn Sie einen View-Ordner verwenden, können Sie die Verwaltung von Pools an einen Administrator mit einer bestimmten Rolle delegieren. Weitere Informationen finden Sie unter „Verwenden von Ordnern für die Verwaltungsdelegierung“, auf Seite 28. **Hinweis** View-Ordner unterscheiden sich von vCenter Server-Ordnern, in denen virtuelle Desktop-Maschinen gespeichert werden. Sie wählen einen vCenter Server-Ordner zusammen mit anderen vCenter Server-Einstellungen an einer späteren Stelle im Assistenten aus.	
Delete or refresh desktop on logoff (Desktop bei Abmeldung löschen oder aktualisieren)	Wenn Sie die dynamische Benutzerzuweisung auswählen, legen Sie fest, ob Desktops nach der Benutzerabmeldung aktualisiert, gelöscht oder unverändert beibehalten werden. **Hinweis** Diese Option wird auf der Seite mit den Pool-Einstellungen festgelegt.	
Pool Settings (Pool-Einstellungen)	Einstellungen, die den Desktop-Status, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen. Eine Beschreibung finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126. Eine Liste der Einstellungen für Linked-Clone-Pools finden Sie unter „Desktop-Einstellungen für Linked-Clone-Desktop-Pools“, auf Seite 97. Weitere Informationen über Betriebsrichtlinien und automatisierte Pools finden Sie unter „Einstellen von Betriebsrichtlinien für Desktop-Pools“, auf Seite 132.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Redirect Windows profile to persistent disks (Windows-Profil auf persistente Festplatten umleiten)	Wenn Sie dedizierte Benutzerzuweisungen auswählen, legen Sie fest, ob Windows-Benutzerprofildaten auf einer separaten persistenten View Composer-Festplatte oder auf derselben Festplatte wie die Betriebssystemdaten abgelegt werden. Separate persistente Festplatten ermöglichen Ihnen das Beibehalten von Benutzerdaten und -einstellungen. View Composer-Aktualisierungen, -Neuzusammenstellungen und Neuverteilungen wirken sich nicht auf persistente Festplatten aus. Sie können eine persistente Festplatte von einem verknüpften Klon trennen und mit einem anderen Desktop verknüpfen. Wenn Sie das Windows-Profil auf der Betriebssystemfestplatte speichern, werden Benutzerdaten und -einstellungen während der Vorgänge zur Aktualisierung, Neuzusammenstellung oder Neuverteilung entfernt.	
Disk size and drive letter for persistent disk (Festplattengröße und Laufwerkbuchstabe für persistente Festplatte)	Wenn Sie Profildaten auf einer separaten persistenten View Composer-Festplatte speichern, geben Sie die Festplattengröße in Megabyte und den Laufwerkbuchstaben an. **Hinweis** Wählen Sie keinen Laufwerkbuchstaben aus, der bereits auf der übergeordneten virtuellen Maschine vorhanden ist oder der einen Konflikt mit einem Laufwerkbuchstaben verursacht, der für ein im Netzwerk bereitgestelltes Laufwerk verwendet wird.	
Disposable File Redirection (Umleitung löschbarer Dateien)	Wählen Sie aus, ob die Auslagerungsdateien und temporären Dateien des Gastbetriebssystems auf eine separate, nicht persistente Festplatte umgeleitet werden sollen. Geben Sie in diesem Fall die Festplattengröße in Megabyte an. Wenn mit dieser Konfiguration ein verknüpfter Klon ausgeschaltet wird, ersetzt View Manager die Festplatte für löschbare Dateien durch eine Kopie der ursprünglichen Festplatte, die mit dem Linked-Clone-Pool erstellt wurde. Verknüpfte Klone können an Größe zunehmen, wenn Benutzer mit ihren Desktops interagieren. Das Umleiten löschbarer Dateien kann Speicherplatz einsparen und so das Wachstum von verknüpften Klonen verlangsamen. Die Festplattengröße sollte die Auslagerungsdateigröße des Gastbetriebssystems übersteigen. Informationen zum Ermitteln der Auslagerungsdateigröße finden Sie unter „Protokollieren der Auslagerungsdateigröße für die übergeordnete virtuelle Maschine“, auf Seite 79. Wenn Sie die Größe der Festplatte für löschbare Dateien konfigurieren, sollten Sie berücksichtigen, dass die tatsächliche Größe einer formatierten Festplattenpartition leicht unter dem Wert liegt, den Sie in View Administrator angeben.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Virtual machine naming (Benennung virtueller Maschinen)	Wählen Sie, ob Desktops durch die manuelle Angabe einer Liste mit Desktop-Namen oder durch Bereitstellung eines Benennungsmusters sowie der Gesamtzahl an Desktops bereitgestellt werden sollen. Weitere Informationen finden Sie unter „Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters“, auf Seite 119.	
List of desktop names (Liste mit Desktop-Namen)	Wenn Sie Namen manuell angeben, bereiten Sie eine Textdatei vor, in der die Desktop-Namen aufgeführt sind. Optional können Sie auch die verknüpften Benutzernamen angeben.	
Naming pattern (Benennungsmuster)	Wenn Sie diese Benennungsmethode verwenden, stellen Sie das Muster bereit. View Manager verwendet Ihr Muster als Präfix in allen Desktop-Namen und hängt eine eindeutige Zahl zur Identifizierung der einzelnen Desktops an. Weitere Informationen finden Sie unter „Verwenden eines Benennungsmusters für automatisierte Desktop-Pools“, auf Seite 122.	
Maximum number of desktops (Maximale Anzahl an Desktops)	Wenn Sie ein Benennungsmuster verwenden, geben Sie die Gesamtzahl an Desktops im Pool an. Außerdem können Sie bei der ersten Erstellung des Pools eine Mindestzahl an bereitzustellenden Desktops angeben.	
Number of spare (powered on) desktops (Anzahl an eingeschalteten Reserve-Desktops)	Wenn Sie Namen manuell angeben oder ein Benennungsmuster verwenden, geben Sie eine Anzahl an Desktops an, die View Manager für neue Benutzer verfügbar und eingeschaltet hält. Weitere Informationen finden Sie unter „Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters“, auf Seite 119. Wenn Sie Namen manuell festlegen, heißt diese Option **[# Unassigned desktops kept powered on (Anzahl an ständig eingeschalteten nicht zugewiesenen Desktops)]** .	
Minimum number of desktops (Mindestanzahl an Desktops)	Wenn Sie ein Benennungsmuster verwenden und Desktops nach Bedarf bereitstellen, geben Sie eine Mindestanzahl an Desktops im Pool an. Wenn Sie Desktops nach Bedarf bereitstellen, erstellt View Manager Desktops, sobald Benutzer sich erstmals am Pool anmelden. View Manager erstellt die Mindestanzahl an Desktops bei der Erstellung des Pools.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Parent virtual machine (Übergeordnete virtuelle Maschine)	Wählen Sie die übergeordnete virtuelle Maschine für den Pool aus. Um in View Manager 4.5 oder einer höheren Version unterstützte Funktionen wie z. B. das Umleiten löschbarer Dateien auf eine separate Festplatte und das Anpassen von Linked-Clone-Desktops mit Sysprep nutzen zu können, müssen Sie eine übergeordnete virtuelle Maschine auswählen, auf der View Agent 4.5 oder höher installiert ist. **Hinweis** Sie können View Composer nicht zur Bereitstellung von Desktops verwenden, auf denen die Windows Vista Ultimate Edition oder Windows XP Professional SP1 ausgeführt wird.	
Default image (snapshot) (Standard-Image (Snapshot))	Wählen Sie den Snapshot der übergeordneten virtuellen Maschine aus, die als das Basis-Image für den Pool eingesetzt werden soll. Löschen Sie den Snapshot und die übergeordnete virtuelle Maschine nur dann aus vCenter Server, wenn keine weiteren verknüpften Klone aus diesem Standard-Image erstellt werden sollen. View Manager benötigt die übergeordnete virtuelle Maschine und den Snapshot, um gemäß den Poolrichtlinien neue verknüpfte Klone im Pool bereitzustellen.	
Publish base image to the Transfer Server repository (Basis-Image im Transfer Server-Repository veröffentlichen)	Wählen Sie diese Option, wenn Sie den Pool zur Bereitstellung lokaler Desktops verwenden. Wird ein lokaler Desktop bereitgestellt, lädt View Transfer Server das Basis-Image vom Transfer Server-Repository auf den Client herunter. Sie können das Basis-Image auch nach Erstellung des Pools veröffentlichen.	
vCenter Server folder (vCenter Server-Ordner)	Wählen Sie den Ordner in vCenter Server aus, in dem der Desktop-Pool gespeichert wird.	
Host or cluster (Host oder Cluster)	Wählen Sie den ESX-Host oder -Cluster aus, in dem die virtuellen Desktop-Maschinen ausgeführt werden.	
Resource pool (Ressourcen-Pool)	Wählen Sie den vCenter Server-Ressourcen-Pool aus, in dem der Desktop-Pool gespeichert ist.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Select Datastores (Datenspeicher auswählen)	Wählen Sie einen oder mehrere Datenspeicher zur Speicherung des Desktop-Pools aus. Eine Tabelle auf der Seite **[Select Datastores (Datenspeicher auswählen)]** im Assistenten zum Hinzufügen von Pools liefert allgemeine Richtlinien zur Ermittlung der Speicheranforderungen für den Pool. Anhand dieser Richtlinien können Sie ermitteln, welche Datenspeicher über ausreichend Kapazität zum Speichern der Linked-Clone-Festplatten verfügen. Weitere Informationen finden Sie unter „Speichergrößen für Linked-Clone-Desktop-Pools“, auf Seite 102. ■ Wenn Sie Benutzerdaten und Betriebssystemdaten auf verschiedenen Festplatten speichern, können Sie die persistenten Festplatten und die Betriebssystemfestplatten in separaten Datenspeichern ablegen. ■ Sie können die Replikat- (Master-) VM in einem Hochleistungsdatenspeicher und die verknüpften Klone in separaten Datenspeichern ablegen. Für Cluster können Sie freigegebene Datenspeicher verwenden. Für einen einzelnen ESXi-Host können Sie freigegebene oder lokale Datenspeicher verwenden. Weitere Informationen zu den Festplatten, die für verknüpfte Klone erstellt werden, finden Sie unter „Datenfestplatten von Linked-Clone-Desktops“, auf Seite 110.	
Storage Overcommit (Speichermehrfachvergabe)	Legen Sie den Grad der Speichermehrfachvergabe fest, mit dem View Manager Linked-Clone-Desktops in den einzelnen Datenspeichern erstellt. Mit steigendem Wert passen mehr verknüpfte Klone in den Datenspeicher, und es wird weniger Speicherplatz für das Anwachsen der einzelnen Klone reserviert. Ein hohes Maß an Speichermehrfachvergabe ermöglicht Ihnen die Erstellung verknüpfter Klone, deren logische Gesamtgröße die physische Speichergrenze des Datenspeichers übertrifft. Weitere Informationen finden Sie unter „Festlegen des Werts für die Speichermehrfachvergabe für Linked-Clone-Desktops“, auf Seite 107.	

Tabelle 5-3. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines Linked-Clone-Desktop-Pools (Fortsetzung)

Option	Beschreibung	Wert
Active Directory domain (Active Directory-Domäne)	Wählen Sie die Active Directory-Domäne und den Benutzernamen aus. View Composer benötigt zum Erstellen eines Linked-Clone-Pools spezielle Benutzerberechtigungen. Das Domänen- und das Benutzerkonto werden von QuickPrep oder Sysprep zum Anpassen der Linked-Clone-Desktops eingesetzt. Weitere Informationen finden Sie unter „Erstellen eines Benutzerkontos für View Composer“, auf Seite 15. Sie geben diesen Benutzer an, wenn Sie View Composer-Einstellungen für vCenter Server konfigurieren. Weitere Informationen finden Sie unter „Konfigurieren von View Composer-Einstellungen für vCenter Server“, auf Seite 15. Sie können mehrere Domänen und Benutzer angeben, wenn Sie die View Composer-Einstellungen konfigurieren. Wenn Sie den Assistenten zum Hinzufügen von Pools zum Erstellen eines Pools verwenden, müssen Sie eine Domäne und einen Benutzer aus der Liste auswählen.	
Active Directory container (Active Directory-Container)	Stellen Sie den RDN (Relative Distinguished Name) des Active Directory-Containers bereit. Beispiel: **`CN=Computers`** Bei der Ausführung des Assistenten Add Pool (Hinzufügen von Pools) können Sie die Active Directory-Struktur nach dem Container durchsuchen.	
Use QuickPrep or a customization specification (Sysprep) (QuickPrep oder eine Anpassungsspezifikation (Sysprep) verwenden)	Wählen Sie, ob Sie QuickPrep verwenden oder eine Anpassungsspezifikation (Sysprep) auswählen möchten, damit View Manager die Lizenzierung, Domänenbindung, DHCP-Einstellungen und andere Eigenschaften auf den Desktops konfiguriert. Sysprep wird nur unter vSphere 4.1 oder höher für verknüpfte Klone unterstützt. Sie können Sysprep nicht zum Anpassen von Linked-Clone-Desktops nutzen, die vSphere 4.0-Software verwenden. Nachdem Sie mithilfe von QuickPrep oder Sysprep einen Pool erstellt haben, können Sie bei einer späteren Erstellung oder Neuzusammenstellung von Desktops im Pool nicht die Anpassungsmethode ändern. Weitere Informationen finden Sie unter „Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Desktops“, auf Seite 99.	
Power-off script (Ausschaltskript)	QuickPrep kann ein Anpassungsskript auf Linked-Clone-Desktops ausführen, bevor diese ausgeschaltet werden. Stellen Sie den Pfad zum Skript auf der übergeordneten virtuellen Maschine bereit.	
Post synchronization script (Nach Synchronisierung ausgeführtes Skript)	QuickPrep kann ein Anpassungsskript auf Linked-Clone-Desktops ausführen, nachdem diese erstellt, neu zusammengestellt und aktualisiert wurden. Stellen Sie den Pfad zum Skript auf der übergeordneten virtuellen Maschine bereit.	

Erstellen eines Linked-Clone-Desktop-Pools

Sie können einen automatisierten Linked-Clone-Desktop-Pool basierend auf einer von Ihnen ausgewählten übergeordneten virtuellen Maschine erstellen. Der View Composer-Dienst erstellt dynamisch für jeden Desktop eine neue virtuelle Linked-Clone-Maschine in vCenter Server.

Informationen zum Erstellen eines automatisierten Pools mit vollständigen virtuellen Maschinen finden Sie unter „Automatisierte Pools mit vollständigen virtuellen Maschinen“, auf Seite 84.

Voraussetzungen

- Stellen sie sicher, dass der View Composer-Dienst in vCenter Server installiert ist und eine View Composer-Datenbank konfiguriert wurde. Weitere Informationen finden Sie im Dokument *Installation von VMware View*.
- Stellen Sie sicher, dass View Composer-Einstellungen für vCenter Server in View Administrator konfiguriert sind. Siehe „Konfigurieren von View Composer-Einstellungen für vCenter Server“, auf Seite 15.
- Stellen Sie sicher, dass Sie auf dem virtuellen ESX-Switch, der für virtuelle Desktop-Maschinen verwendet wird, über eine ausreichende Anzahl an Ports verfügen. Der Standardwert reicht möglicherweise nicht aus, wenn Sie große Desktop-Pools erstellen. Die Anzahl der Ports für den virtuellen Switch auf dem ESX-Host muss der Anzahl der virtuellen Desktop-Maschinen multipliziert mit der Anzahl der virtuellen Netzwerkkarten pro virtueller Maschine entsprechen (oder diese übersteigen).
- Stellen Sie sicher, dass Sie eine übergeordnete virtuelle Maschine vorbereitet haben. View Agent muss auf der übergeordneten virtuellen Maschine installiert sein. Siehe Kapitel 4, „Erstellen und Vorbereiten virtueller Maschinen“, auf Seite 51.
- Erstellen Sie einen Snapshot der übergeordneten virtuellen Maschine in vCenter Server. Vor dem Erstellen des Snapshots müssen Sie die übergeordnete virtuelle Maschine herunterfahren. View Composer verwendet den Snapshot als Basis-Image, von dem die Klone erstellt werden.

  Hinweis Sie können aus einer Vorlage für virtuelle Maschinen keinen Linked-Clone-Pool erstellen.

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe „Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools“, auf Seite 89.
- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe „Desktop- und Pool-Einstellungen“, auf Seite 126.

Wichtig Während der Erstellung eines Linked-Clone-Pools sollten Sie die übergeordnete virtuelle Maschine in vCenter Server nicht ändern. Konvertieren Sie beispielsweise nicht die übergeordnete virtuelle Maschine in eine Vorlage. Für den View Composer-Dienst muss die übergeordnete virtuelle Maschine während der Pool-Erstellung in einem statischen, unveränderten Zustand bleiben.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Klicken Sie auf **[Add (Hinzufügen)]** .

3 Wählen Sie **[Automated Pool (Automatisierter Pool)]** aus.

4 Wählen Sie auf der Seite vCenter Server die Option **[View Composer linked clones (Verknüpfte View Composer-Klone)]** .

5 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

  Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

Sie müssen auf der Seite **[vCenter Settings (vCenter-Einstellungen)]** auf **[Browse (Durchsuchen)]** klicken und nacheinander alle vCenter Server-Einstellungen auswählen. Es ist nicht möglich, eine vCenter Server-Einstellung zu überspringen:

a Default image (Standard-Image)

b Virtual machine folder (Ordner für virtuelle Maschinen)

c Host or cluster (Host oder Cluster)

d Resource pool (Ressourcen-Pool)

e Datastores (Datenspeicher)

In View Administrator können Sie die Desktops so anzeigen, wie sie dem Pool hinzugefügt werden. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Desktops]** .

Die verknüpften Klone werden möglicherweise während ihrer Bereitstellung mehrmals neu gestartet.

View Composer erstellt außerdem eine Replikat-VM, die als das Master-Image für die Bereitstellung der verknüpften Klone dient. Um den Speicherplatzbedarf zu reduzieren, wird das Replikat als Thin-Festplatte erstellt. Werden alle Desktops neu zusammengestellt oder gelöscht und sind keine Klone mit dem Replikat verknüpft, wird die Replikat-VM von vCenter Server gelöscht.

Wenn Sie das Replikat nicht in einem separaten Datenspeicher speichern, erstellt View Composer ein Replikat in jedem Datenspeicher, in dem verknüpfte Klone erstellt werden.

Wenn Sie das Replikat in einem separaten Datenspeicher speichern, wird ein Replikat für den gesamten Pool erstellt, selbst wenn verknüpfte Klone in mehreren Datenspeichern erstellt werden.

Weiter

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139.

Desktop-Einstellungen für Linked-Clone-Desktop-Pools

Bei der Konfiguration automatisierter Pools mit Linked-Clone-Desktops, die über View Composer erstellt wurden, müssen Sie Desktop- und Pool-Einstellungen angeben. Für Pools mit dedizierten Benutzerzuweisungen und dynamischen Benutzerzuweisungen gelten unterschiedliche Einstellungen.

Tabelle 5-4 werden die Einstellungen aufgeführt, die für Linked-Clone-Pools mit dedizierten Zuweisungen und dynamischen Zuweisungen gelten.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126.

Tabelle 5-4. Einstellungen für automatisierte Linked-Clone-Desktop-Pools

Einstellung	Linked-Clone-Pool, dedizierte Zuweisung	Linked-Clone-Pool, dynamische Zuweisung
State (Status)	Ja	Ja
Connection Server Restrictions (Einschränkungen für Connection Server)	Ja	Ja
Betriebsrichtlinie für Remote-Desktops	Ja	Ja
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	Ja	Ja
Allow users to reset their desktops (Benutzern das Zurücksetzen ihrer Desktops gestatten)	Ja	Ja

Tabelle 5-4. Einstellungen für automatisierte Linked-Clone-Desktop-Pools (Fortsetzung)

Einstellung	Linked-Clone-Pool, dedizierte Zuweisung	Linked-Clone-Pool, dynamische Zuweisung
Allow multiple sessions per user (Mehrere Sitzungen pro Benutzer zulassen)		Ja
Delete or refresh desktop on logoff (Desktop bei Abmeldung löschen oder aktualisieren)		Ja
Refresh OS disk after logoff (Betriebssystemfestplatte nach Abmelden aktualisieren)	Ja	
Default display protocol (Standardanzeigeprotokoll)	Ja	Ja
Allow users to choose a protocol (Benutzern die Wahl des Protokolls erlauben)	Ja	Ja
Windows 7-3D-Rendering	Ja	Ja
Max number of monitors (Maximale Anzahl an Monitoren)	Ja	Ja
Max resolution of any one monitor (Max. Auflösung eines Monitors)	Ja	Ja
Adobe Flash quality (Adobe Flash-Qualität)	Ja	Ja
Adobe Flash throttling (Adobe Flash-Drosselung)	Ja	Ja

View Composer-Unterstützung für Linked-Clone-SIDs und Drittanbieteranwendungen

View Composer kann in einigen Situationen lokale Computer-SIDs für virtuelle Linked-Clone-Maschinen generieren und beibehalten. View Composer kann GUIDs von Drittanbieteranwendungen abhängig davon beibehalten, wie diese GUIDs von den Anwendungen generiert werden.

Um zu verstehen, wie View Composer-Vorgänge sich auf SIDs und Anwendungs-GUIDs auswirken, müssen Sie wissen, wie Linked-Clone-Desktops erstellt und bereitgestellt werden:

1 View Composer erstellt einen verknüpften Klon anhand dieser Schritte:

   a Erstellung des Replikats, indem der übergeordnete VM-Snapshot geklont wird.

   b Erstellung des verknüpften Klons, der als übergeordnete Festplatte das Replikat referenziert.

2 View Composer und View Manager passen den verknüpften Klon mit QuickPrep bzw. einer Sysprep-Anpassungsspezifikation an, je nachdem, welches Anpassungstool Sie beim Erstellen des Pools auswählen.

   - Wenn Sie Sysprep wählen, wird für jeden Klon eine eindeutige SID generiert.
   - Wenn Sie QuickPrep einsetzen, wird keine neue SID generiert. Die SID der übergeordneten virtuellen Maschine wird auf allen bereitgestellten Linked-Clone-Desktops im Pool repliziert.
   - Einige Anwendungen generieren während der Anpassung eine GUID.

3 View Manager erstellt einen Snapshot des verknüpften Klons.

   Der Snapshot enthält die eindeutige SID, die über Sysprep generiert wurde, bzw. die gemeinsame SID, die über QuickPrep generiert wurde.

4 View Manager schaltet den Desktop entsprechend den von Ihnen beim Erstellen des Pools ausgewählten Einstellungen ein.

   Einige Anwendungen generieren eine GUID, wenn der Desktop erstmals eingeschaltet wird.

Einen Vergleich zwischen der QuickPrep- und der Sysprep-Anpassung finden Sie unter „Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Desktops“, auf Seite 99.

Wenn Sie den verknüpften Klon aktualisieren, verwendet View Composer den Snapshot zum Wiederherstellen des Klons in seinem anfänglichen Zustand. Die SID wird beibehalten.

Wenn Sie QuickPrep verwenden und den verknüpften Klon erneut zusammenstellen, bleibt die SID der übergeordneten virtuellen Maschine im verknüpften Klon erhalten, sofern Sie dieselbe übergeordnete virtuelle Maschine für die Neuzusammenstellung auswählen. Wenn Sie für die Neuzusammenstellung eine andere übergeordnete virtuelle Maschine auswählen, wird die SID der neuen übergeordneten Maschine auf dem Klon repliziert.

Wenn Sie Sysprep wählen, wird für den Klon immer eine neue SID generiert. Weitere Informationen finden Sie unter „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“, auf Seite 102.

Tabelle 5-5 zeigt die Auswirkungen von View Composer-Vorgängen auf Linked-Clone-SIDs und die GUIDs von Drittanbieteranwendungen.

Tabelle 5-5. View Composer-Vorgänge, Linked-Clone-SIDs und Anwendungs-GUIDs

Unterstützung für SIDs oder GUIDs	Klonerstellung	Aktualisierung	Neuzusammenstellung
Sysprep: Eindeutige SIDs für verknüpfte Klone	Bei der Sysprep-Anpassung werden eindeutige SIDs für verknüpfte Klone generiert.	Eindeutige SIDs bleiben erhalten.	Eindeutige SIDs bleiben nicht erhalten.
QuickPrep: Gemeinsame SIDs für verknüpfte Klone	Bei der QuickPrep-Anpassung wird für alle Klone in einem Pool eine gemeinsame SID generiert.	Gemeinsame SID wird beibehalten.	Gemeinsame SID wird beibehalten.
GUIDs von Drittanbieteranwendungen	Jede Anwendung verhält sich anders. HINWEIS Sysprep und QuickPrep besitzen dieselben Auswirkungen auf den Erhalt von GUIDs.	Die GUID bleibt erhalten, wenn eine Anwendung die GUID vor der Erstellung des anfänglichen Snapshots generiert. Die GUID bleibt nicht erhalten, wenn eine Anwendung die GUID erst nach Erstellung des anfänglichen Snapshots generiert.	Bei Neuzusammenstellungen bleibt eine Anwendungs-GUID nur dann erhalten, wenn die Anwendung die GUID auf das Laufwerk schreibt, das als persistente View Composer-Festplatte angegeben wurde.

Wählen von QuickPrep oder Sysprep zum Anpassen von Linked-Clone-Desktops

QuickPrep und Microsoft Sysprep bieten verschiedene Ansätze zum Anpassen von Linked-Clone-Desktops. QuickPrep wurde für eine effiziente Zusammenarbeit mit View Composer konzipiert. Microsoft Sysprep stellt Standard-Tools zur Anpassung bereit.

Bei der Erstellung von Linked-Clone-Desktops müssen Sie die einzelnen virtuellen Maschinen so bearbeiten, dass sie als eindeutige Computer im Netzwerk verwendet werden können. View Manager und View Composer bieten zwei Methoden zur Personalisierung von Linked-Clone-Desktops.

Tabelle 5-6 vergleicht QuickPrep mit Anpassungsspezifikationen, die mit Microsoft Sysprep erstellt werden.

Sysprep wird nur unter vSphere 4.1 oder höher für verknüpfte Klone unterstützt. Sie können Sysprep nicht zum Anpassen von Linked-Clone-Desktops nutzen, die vSphere 4.0-Software verwenden.

Tabelle 5-6. Vergleichen von QuickPrep und Microsoft Sysprep

QuickPrep	Anpassungsspezifikation (Sysprep)
Für die Zusammenarbeit mit View Composer ausgelegt. Weitere Informationen finden Sie unter „Anpassen von Linked-Clone-Desktops mit QuickPrep“, auf Seite 100.	Kann mit den Standard-Tools von Microsoft Sysprep erstellt werden.
Verwendet dieselbe Sicherheits-ID (SID) für lokale Computer für alle verknüpften Klone im Pool.	Generiert eine eindeutige SID für lokale Computer für jeden verknüpften Klon im Pool.
Kann zusätzliche Anpassungsskripts ausführen, bevor verknüpfte Klone ausgeschaltet und nachdem verknüpfte Klone erstellt, aktualisiert oder neu zusammengestellt werden.	Kann bei der ersten Anmeldung des Benutzers ein zusätzliches Skript ausführen.
Nimmt den Linked-Clone-Computer in die Active Directory-Domäne auf.	Nimmt den Linked-Clone-Computer in die Active Directory-Domäne auf. Die Domänen- und Administratorinformationen in der Sysprep-Anpassungsspezifikation werden nicht verwendet. Die virtuelle Maschine wird anhand der Gastanpassungsinformationen der Domäne hinzugefügt, die Sie in View Administrator beim Erstellen des Pools eingeben.
Für jeden verknüpften Klon wird dem Active Directory-Domänenkonto eine eindeutige ID hinzugefügt.	Für jeden verknüpften Klon wird dem Active Directory-Domänenkonto eine eindeutige ID hinzugefügt.
Generiert keine neue SID nach dem Aktualisieren verknüpfter Klone. Die gemeinsame SID bleibt erhalten.	Generiert eine neue SID, sobald die einzelnen verknüpften Klone angepasst werden. Erhält die eindeutigen SIDs während eines Aktualisierungsvorgangs, jedoch nicht während einer Neuzusammenstellung oder Neuverteilung.
Generiert keine neue SID nach dem Neuzusammenstellen verknüpfter Klone. Die gemeinsame SID bleibt erhalten.	Wird nach der Neuzusammenstellung verknüpfter Klone erneut ausgeführt und generiert neue SIDs für die virtuellen Maschinen. Weitere Informationen finden Sie unter „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“, auf Seite 102.
Wird schneller als Sysprep ausgeführt.	Kann längere Zeit benötigen als QuickPrep.

Nach der Anpassung eines Linked-Clone-Pools mit QuickPrep oder Sysprep können Sie nicht zur anderen Anpassungsmethode wechseln, wenn Sie Desktops im Pool erstellen oder neu zusammenstellen.

Anpassen von Linked-Clone-Desktops mit QuickPrep

Sie können die durch eine übergeordnete virtuelle Maschine erstellten Linked-Clone-Desktops über das System-Tool QuickPrep persönlich anpassen. View Composer führt QuickPrep aus, sobald ein Linked-Clone-Desktop erstellt oder neu zusammengestellt wird.

QuickPrep passt einen Linked-Clone-Desktop auf verschiedene Weise an:

- Zuweisen eines Namens für den Computer, den Sie bei der Erstellung des Linked-Clone-Pools angeben.
- Erstellen eines Computerkontos in Active Directory und Aufnehmen des Computers in die geeignete Domäne.
- Bereitstellen der persistenten View Composer-Festplatte. Das Windows-Benutzerprofil wird auf diese Festplatte umgeleitet.
- Umleiten von temporären und Auslagerungsdateien auf eine separate Festplatte.

Für diese Schritte müssen die verknüpften Klone möglicherweise einmal oder mehrmals neu gestartet werden.

QuickPrep verwendet die KMS-Volumenlizenzschlüssel zum Aktivieren von Windows 7- und Windows Vista-Linked-Clone-Desktops. Weitere Informationen finden Sie unter „Aktivieren von Windows 7 und Windows Vista auf Linked-Clone-Desktops“, auf Seite 77.

Sie können Ihre eigenen Skripts zur weiteren Anpassung der verknüpften Klone erstellen. QuickPrep kann zwei Typen von Skripts zu vordefinierten Zeitpunkten ausführen:

- Nach der Erstellung oder Neuzusammenstellung verknüpfter Klone
- Unmittelbar vor dem Ausschalten verknüpfter Klone

Richtlinien und Regeln für die Verwendung von QuickPrep-Anpassungsskripts finden Sie unter „Ausführen von QuickPrep-Anpassungsskripts“, auf Seite 101.

Hinweis View Composer erfordert Anmeldeinformationen von Domänenbenutzern, um Linked-Clone-Desktops in eine Active Directory-Domäne aufzunehmen. Weitere Informationen finden Sie unter „Erstellen eines Benutzerkontos für View Composer“, auf Seite 15.

Ausführen von QuickPrep-Anpassungsskripts

Mit dem QuickPrep-Tool können Sie Skripts zur Anpassung der in einem Pool enthaltenen Linked-Clone-Desktops erstellen. Sie können QuickPrep so konfigurieren, dass Anpassungsskripts zu zwei vordefinierten Zeitpunkten ausgeführt werden.

Wann werden QuickPrep-Skripts ausgeführt?

Das nach der Synchronisierung ausgeführte Skript wird nach der Erstellung, Neuzusammenstellung oder Neuverteilung von verknüpften Klonen eingesetzt, wenn sich die Klone im Status **[Ready (Bereit)]** befinden. Das Abschaltskript wird ausgeführt, bevor verknüpfte Klone ausgeschaltet werden. Die Skripts werden in den Gastbetriebssystemen der verknüpften Klone ausgeführt.

Wie werden QuickPrep-Skripts ausgeführt?

Der QuickPrep-Prozess verwendet die Windows-API `CreateProcess` zum Ausführen von Skripts. Ihr Skript kann einen beliebigen Prozess starten, der mit der `CreateProcess`-API erstellt werden kann. Beispielsweise arbeiten `cmd`, `vbscript`, `exe` und Batch-Dateiprozesse mit der API zusammen.

Bei Ausführung des Skripts übergibt QuickPrep den für das Skript angegebenen Pfad als zweiten Parameter an die `CreateProcess`-API und legt den ersten Parameter auf `NULL` fest.

Wenn der Skriptpfad beispielsweise `C:\MeinSkript.cmd` lautet, erscheint der Pfad in der View Composer-Protokolldatei als zweiter Parameter in der Funktion: `CreateProcess(NULL,C:\MeinSkript.cmd,...)`.

Bereitstellen von Pfaden für QuickPrep-Skripts

Sie stellen den QuickPrep-Anpassungsskripts Pfade bereit, wenn Sie einen Linked-Clone-Desktop-Pool erstellen oder die Gastanpassungseinstellungen für einen Pool bearbeiten. Die Skripts müssen auf der übergeordneten virtuellen Maschine gespeichert sein. Sie können keinen UNC-Pfad zu einer Netzwerkfreigabe verwenden.

Wenn Sie eine Skriptsprache verwenden, die zur Skriptausführung einen Interpreter erfordert, muss der Skriptpfad mit der Interpreter-Binärdatei beginnen.

Wenn Sie beispielsweise den Pfad `C:\script\myvb.vbs` als QuickPrep-Anpassungsskript angeben, kann View Composer Agent das Skript nicht ausführen. Sie müssen einen Pfad angeben, der mit der Interpreter-Binärdatei beginnt:

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

Zeitüberschreitungslimits für QuickPrep-Skripts

View Composer beendet ein nach der Synchronisierung ausgeführtes Skript oder ein Abschaltskript, wenn dessen Ausführung länger als 20 Sekunden dauert. Wenn Ihr Skript länger als 20 Sekunden ausgeführt wird, können Sie das Limit für die Zeitüberschreitung erhöhen. Weitere Informationen finden Sie unter „Erhöhen des Zeitüberschreitungslimits für QuickPrep-Anpassungsskripts“, auf Seite 80.

Alternativ dazu können Sie mit Ihrem Skript ein weiteres Skript oder einen Prozess starten, durch das bzw. den die Aufgabe mit langer Laufzeit durchgeführt wird.

Konto für die Ausführung von QuickPrep-Skripts

QuickPrep führt die Skripts mit dem Konto aus, das zur Ausführung des VMware View Composer Gastagentserver-Dienstes konfiguriert ist. Standardmäßig handelt es sich hier um das Konto `Local System (Lokales System)`.

Ändern Sie dieses Anmeldekonto nicht. Wenn Sie das Konto ändern, können die verknüpften Klone nicht starten.

Protokolle zu QuickPrep-Skripts

View Composer-Protokolle enthalten Informationen zur Ausführung von QuickPrep-Skripts. Das Protokoll zeichnet den Start und das Ende der Skriptausführung auf und protokolliert Ausgabe- oder Fehlermeldungen. Das Protokoll befindet sich im Windows-Verzeichnis `Temp`:

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen

Wenn Sie einen mit Sysprep angepassten Linked-Clone-Desktop neu zusammenstellen, führt View Manager die Sysprep-Anpassungsspezifikation erneut aus, nachdem die Betriebssystemfestplatte neu zusammengestellt wurde. Durch diesen Vorgang wird eine neue SID für die virtuelle Linked-Clone-Maschine generiert.

Wird eine neue SID generiert, fungiert der neu zusammengestellte verknüpfte Klon als neuer Computer im Netzwerk. Einige Softwareprogramme wie Tools zur Systemverwaltung verwenden die SID zum Identifizieren der von ihnen verwalteten Computer. Diese Programme können die virtuelle Linked-Clone-Maschine möglicherweise nicht identifizieren oder finden.

Wenn auf der Systemfestplatte außerdem eine Drittanbietersoftware installiert ist, werden die GUIDs für die jeweilige Software nach der Neuzusammenstellung möglicherweise durch die Anpassungsspezifikation neu generiert.

Durch eine Neuzusammenstellung wird der verknüpfte Klon in seinen ursprünglichen Zustand vor der ersten Ausführung der Anpassungsspezifikation zurückversetzt. In diesem Zustand besitzt der verknüpfte Klon keine lokale Computer-SID oder die GUID einer auf dem Systemlaufwerk installierten Drittanbietersoftware. View Manager muss die Sysprep-Anpassungsspezifikation ausführen, nachdem der verknüpfte Klon neu zusammengestellt wird.

Speichergrößen für Linked-Clone-Desktop-Pools

View Manager stellt grundlegende Richtlinien bereit, mit deren Hilfe Sie bestimmen können, wie viel Speicherplatz für einen Linked-Clone-Desktop-Pool benötigt wird. Eine Tabelle im Assistenten zum Hinzufügen von Pools zeigt eine allgemeine Schätzung der Speicheranforderungen für die Linked-Clone-Festplatten, wenn der Pool erstellt wird und die verknüpften Klone mit der Zeit an Größe zunehmen.

Die Tabelle zu den Speichergrößen zeigt außerdem den freien Speicherplatz in den Datenspeichern an, die Sie zum Speichern von Betriebssystemfestplatten, persistenten View Composer-Festplatten und Replikaten ausgewählt haben. Sie können entscheiden, welche Datenspeicher Sie verwenden sollten, indem Sie den tatsächlichen freien Speicherplatz mit den geschätzten Anforderungen für die Linked-Clone-Festplatten vergleichen.

Die von View Manager verwendeten Formeln stellen lediglich eine allgemeine Schätzung zur Speicherverwendung dar. Das tatsächliche Wachstum Ihrer verknüpften Klone hängt von zahlreichen Faktoren ab:

- Menge des Arbeitsspeichers, der der übergeordneten virtuellen Maschine zugeordnet ist
- Häufigkeit von Aktualisierungen
- Größe der Auslagerungsdatei des Gastbetriebssystems
- Keine Umleitung/Umleitung von Auslagerungsdateien und temporären Dateien auf eine separate Festplatte
- Keine Konfiguration/Konfiguration separater persistenter View Composer-Festplatten
- Arbeitslast der Linked-Clone-Desktops, primär bestimmt durch die Anwendungstypen, die Benutzer im Gastbetriebssystem ausführen

HINWEIS In einer Bereitstellung, die Hunderte oder Tausende von verknüpften Klonen umfasst, sollten Sie Ihre Linked-Clone-Pools so konfigurieren, dass bestimmte Datenspeichersätze dediziert für bestimmte ESX-Cluster verwendet werden. Konfigurieren Sie Pools nicht wahllos über alle Datenspeicher, sodass die meisten oder alle ESX-Host auf zahlreiche oder alle LUNs zugreifen müssen.

Wenn zu viele ESX-Hosts versuchen, Schreibvorgänge auf Linked-Clone-Betriebssystemfestplatten auf einer bestimmten LUN auszuführen, können Konflikte auftreten, die eine Beeinträchtigung der Leistung und Skalierbarkeit zur Folge haben können. Weitere Informationen zur Datenspeicherplanung in großen Bereitstellungen finden Sie im Dokument *Planung der VMware View-Architektur*.

Größenrichtlinien für Linked-Clone-Pools

Wenn Sie einen Linked-Clone-Desktop-Pool erstellen oder bearbeiten, wird auf der Seite **[Select Datastores (Datenspeicher auswählen)]** eine Tabelle mit Richtlinien für die Datenspeichergröße angezeigt. Anhand dieser Tabelle können Sie einfacher entscheiden, welche Datenspeicher Sie für die Linked-Clone-Festplatten auswählen sollten.

Größenrichtlinien für Linked-Clone-Festplatten

Tabelle 5-7 zeigt ein Beispiel mit Empfehlungen für die Speichergrößen, die für einen Pool mit 10 virtuellen Maschinen angezeigt werden können, wenn die übergeordnete virtuelle Maschine einen Arbeitsspeicher von 1 GB und ein Replikat mit 10 GB aufweist. In diesem Beispiel werden unterschiedliche Datenspeicher für Betriebssystemfestplatten und persistente View Composer-Festplatten ausgewählt.

Tabelle 5-7. Tabelle mit Größenrichtlinien für Linked-Clone-Festplatten

Datentyp	Ausgewählter freier Speicherplatz (GB)	Mind. empfohlen (GB)	50% Auslastung (GB)	Max. empfohlen (GB)
Betriebssystemfestplatten	184.23	40.00	80.00	130.00
Persistent disks (Persistente Festplatten)	28.56	4.00	10.00	20.00

Die Spalte **[Selected Free Space (Ausgewählter freier Speicherplatz)]** zeigt den insgesamt verfügbaren Speicherplatz in allen Datenspeichern an, die Sie für einen Festplattentyp wie z.B. Betriebssystemfestplatten ausgewählt haben.

Die Spalte **[Min Recommended (Mind. empfohlen)]** zeigt die mindestens empfohlene Menge an Speicherplatz für einen Pool.

Die Spalte **[50% Utilization (50% Auslastung)]** zeigt die empfohlene Speicherplatzmenge, wenn die Linked-Clone-Festplatten auf eine Größe von 50% der übergeordneten virtuellen Maschine anwachsen.

Die Spalte **[Max Recommended (Max. empfohlen)]** zeigt die empfohlene Speicherplatzmenge, wenn die Linked-Clone-Festplatten die vollständige Größe der übergeordneten virtuellen Maschine erreichen.

Wenn Sie Betriebssystemfestplatten und persistente Festplatten im selben Datenspeicher ablegen, berechnet View Manager die Speicheranforderungen beider Festplattentypen. Als **[Data Type (Datentyp)]** wird anstelle eines bestimmten Festplattentyps der Wert **[Linked clones (Verknüpfte Klone)]** angezeigt.

Wenn Sie View Composer-Replikate in einem separaten Datenspeicher speichern, zeigt die Tabelle auch Speicherempfehlungen für die Replikate und passt die Empfehlungen für Betriebssystemfestplatten an.

Größenrichtlinien

Die Tabelle liefert allgemeine Richtlinien. Für die Speicherberechnung müssen Sie zusätzliche Faktoren berücksichtigen, die sich auf das tatsächliche Speicherwachstum im Linked-Clone-Pool auswirken können.

Für Betriebssystemfestplatten richtet sich die Größeneinschätzung danach, wie häufig Sie den Pool aktualisieren und neu zusammenstellen.

Wenn Sie Ihren Linked-Clone-Pool zwischen einmal täglich und einmal wöchentlich aktualisieren, stellen Sie sicher, dass für **[Selected Free Space (Ausgewählter freier Speicherplatz)]** eine Speicherbelegung möglich ist, die zwischen **[Min Recommended (Mind. empfohlen)]** und **[50% Utilization (50% Auslastung)]** liegt.

Wenn Sie den Pool nur selten aktualisieren oder neu erstellen, wachsen die Linked-Clone-Festplatten weiter an. Stellen Sie sicher, dass für **[Selected Free Space (Ausgewählter freier Speicherplatz)]** eine Speicherbelegung möglich ist, die zwischen **[50% Utilization (50% Auslastung)]** und **[Max Recommended (Max. empfohlen)]** liegt.

Für persistente Festplatten richtet sich die Größeneinschätzung nach der Menge der Windows-Profildaten, die Benutzer auf ihren Desktops generieren. Aktualisierungen und Neuzusammenstellungen wirken sich nicht auf persistente Festplatten aus.

Berechnung der Empfehlungen für die Mindestgröße durch View Manager

Um eine Mindestempfehlung für Betriebssystemfestplatten ausgeben zu können, geht View Manager bei der anfänglichen Erstellung und Inbetriebnahme davon aus, dass jeder Klon die zweifache Größe seines Arbeitsspeichers belegt. Wenn kein Arbeitsspeicher für einen Klon reserviert ist, wird eine ESX-Auslagerungsdatei für den Klon erstellt, sobald dieser eingeschaltet wird. Die Größe der Auslagerungsdatei des Gastbetriebssystems wirkt sich ebenfalls auf das Wachstum einer Betriebssystemfestplatte für einen Klon aus.

Bei den Mindestempfehlungen für Betriebssystemfestplatten schließt View Manager auch Speicherplatz für zwei Replikate in jedem Datenspeicher ein. View Composer erstellt ein Replikat, wenn ein Pool erstellt wird. Wenn der Pool zum ersten Mal neu zusammengestellt wird, erstellt View Composer ein zweites Replikat im Datenspeicher, verknüpft die verknüpften Klone mit dem neuen Replikat und löscht das erste Replikat, wenn keiner der Klone den ursprünglichen Snapshot verwendet. Der Datenspeicher muss während der Neuzusammenstellung über die Kapazität zum Speichern der zwei Replikate verfügen.

Standardmäßig verwenden Replikate vSphere Thin-Provisioning, um jedoch die Richtlinien einfach zu halten, geht View Manager von zwei Replikaten aus, die denselben Speicherplatz belegen wie die übergeordnete virtuelle Maschine.

Um eine Mindestempfehlung für persistente Festplatten ausgeben zu können, geht View Manager von 20% der Festplattengröße aus, die Sie auf der Seite **[View Composer Disks (View Composer-Festplatten)]** im Assistenten zum Hinzufügen von Pools angegeben haben.

Hinweis Die Berechnungen für persistente Festplatten basieren auf statischen Schwellenwerten (in Gigabyte). Wenn Sie beispielsweise eine persistente Festplatte mit einer Größe zwischen 1024 MB und 2047 MB festlegen, berechnet View Manager die Größe der persistenten Festplatte als 1 GB. Wenn Sie eine Festplattengröße von 2048 MB festlegen, berechnet View Manager die Festplattengröße als 2 GB.

Um eine Mindestempfehlung für das Speichern von Replikaten in einem separaten Datenspeicher ausgeben zu können, setzt View Manager Speicherplatz für zwei Replikate im Datenspeicher an. Für die Mindest- und Höchstauslastung wird derselbe Wert berechnet.

Weitere Informationen finden Sie unter „Größenformeln für Linked-Clone-Pools“, auf Seite 105.

Größenrichtlinien und Speichermehrfachvergabe

Nachdem Sie die Speicheranforderungen geschätzt, Datenspeicher ausgewählt und den Pool bereitgestellt haben, stellt View Manager basierend auf dem freien Speicherplatz und den vorhandenen Klonen in jedem Datenspeicher Linked-Clone-VMs in verschiedenen Datenspeichern bereit.

Abhängig von der Option für die Speichermehrfachvergabe, die Sie auf der Seite **[Select Datastores (Datenspeicher auswählen)]** im Assistenten für das Hinzufügen von Pools ausgewählt haben, stellt View Manager die Bereitstellung neuer Klone ein und reserviert freien Speicherplatz für vorhandene Klone. Durch dieses Verhalten wird sichergestellt, dass ein Wachstumspuffer für jeden Desktop im Datenspeicher vorhanden ist.

Wenn Sie einen sehr hohen Wert für die Speichermehrfachvergabe wählen, übersteigen die geschätzten Speicheranforderungen möglicherweise in der Spalte **[Selected Free Space (Ausgewählter freier Speicherplatz)]** angezeigte Kapazität. Der Grad der Speichermehrfachvergabe wirkt sich darauf aus, wie viele virtuelle Maschinen View Manager tatsächlich in einem Datenspeicher erstellt.

Weitere Informationen finden Sie unter „Festlegen des Werts für die Speichermehrfachvergabe für Linked-Clone-Desktops“, auf Seite 107.

Größenformeln für Linked-Clone-Pools

Formeln für die Berechnung von Speichergrößen unterstützen Sie dabei, die Größe von Linked-Clone-Festplatten in Relation zum freien Speicherplatz in den Datenspeichern zu ermitteln, die Sie für Betriebssystemfestplatten, persistente View Composer-Festplatten und Replikate ausgewählt haben.

Formeln zur Berechnung der Speichergrößen

Tabelle 5-8 zeigt die Formeln zur Berechnung der geschätzten Größen von Linked-Clone-Festplatten, wenn Sie einen Pool erstellen und die Linked-Clone-Desktops im Laufe der Zeit an Größe zunehmen. Diese Formeln beziehen den Speicherplatz für Replikatfestplatten ein, die mit den Klonen im Datenspeicher abgelegt werden.

Wenn Sie einen vorhandenen Pool bearbeiten oder Replikate in einem separaten Datenspeicher ablegen, verwendet View Manager eine andere Formel für die Größenberechnung. Siehe „Formeln zur Größenberechnung von verknüpften Klonen beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern“, auf Seite 106.

Tabelle 5-8. Formeln zur Berechnung der Speichergrößen für Linked-Clone-Festplatten in ausgewählten Datenspeichern

Datentyp	Ausgewählter freier Speicherplatz (GB)	Mind. empfohlen (GB)	50% Auslastung (GB)	Max. empfohlen (GB)
Betriebssystemfestplatten	Freier Speicherplatz in den ausgewählten Datenspeichern	Anzahl der VMs * (2 * Arbeitsspeicher der VM) + (2 * Replikatfestplatte)	Anzahl der VMs * (50% der Replikatfestplatte + Arbeitsspeicher der VM) + (2 * Replikatfestplatte)	Anzahl der VMs * (100% der Replikatfestplatte + Arbeitsspeicher der VM) + (2 * Replikatfestplatte)
Persistent disks (Persistente Festplatten)	Freier Speicherplatz in den ausgewählten Datenspeichern	Anzahl der VMs * 20% der persistenten Festplatte	Anzahl der VMs * 50% der persistenten Festplatte	Anzahl der VMs * 100% der persistenten Festplatte

Beispiel für eine geschätzte Speichergröße

In diesem Beispiel wird die übergeordnete virtuelle Maschine mit einem Arbeitsspeicher von 1 GB konfiguriert. Die Festplatte der übergeordneten virtuellen Maschine ist 10 GB groß. Es wird ein Linked-Clone-Pool mit 10 Desktops erstellt. Die Größe der persistenten Festplatten wird auf 2048 MB festgelegt.

Die Betriebssystemfestplatten werden in einem Datenspeicher konfiguriert, der derzeit über 184,23 GB freien Speicherplatz verfügt. Die persistenten Festplatten werden in einem anderen Datenspeicher mit 28,56 GB freiem Speicherplatz konfiguriert.

Tabelle 5-9 zeigt, wie mithilfe der Formeln zur Größenberechnung die geschätzten Speicheranforderungen für den beispielhaften Linked-Clone-Pool ermittelt werden.

Tabelle 5-9. Beispiel einer geschätzten Speichergröße für Linked-Clone-Desktops in ausgewählten Datenspeichern

Datentyp	Ausgewählter freier Speicherplatz (GB)	Mind. empfohlen (GB)	50% Auslastung (GB)	Max. empfohlen (GB)
Betriebssystemfestplatten	184,23	10 * (2 * 1 GB) + (2 * 10 GB) = 40.00	10 * (50% von 10 GB + 1 GB) + (2 * 10 GB) = 80,00	10 * (100% von 10 GB + 1 GB) + (2 * 10 GB) = 130,00
Persistent disks (Persistente Festplatten)	28.56	10 * (20% von 2 GB) = 4,00	10 * (50% von 2 GB) = 10,00	10 * (100% von 2 GB) = 20,00

Formeln zur Größenberechnung von verknüpften Klonen beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

View Manager verwendet bei der Bearbeitung vorhandener Linked-Clone-Pool oder der Speicherung von Replikaten in einem separaten Datenspeicher andere Formeln zur Größenberechnung als bei der anfänglichen Erstellung eines Pools.

Wenn Sie einen vorhandenen Pool bearbeiten und Datenspeicher für den Pool auswählen, erstellt View Composer neue Klone in den ausgewählten Datenspeichern. Die neuen Klone werden mit dem vorhandenen Snapshot verknüpft und verwenden die vorhandene Replikatfestplatte. Es werden keine neuen Replikate erstellt.

Wenn Sie Replikate in einem separaten Datenspeicher ablegen, werden die weiteren ausgewählten Datenspeicher dediziert für Linked-Clone-Festplatten verwendet.

In diesen Fällen bezieht View Manager keinen Speicherplatz für Replikate ein, wenn die Speicherempfehlungen für Linked-Clone-Festplatten berechnet werden.

Tabelle 5-10 zeigt die Formeln zur Berechnung der geschätzten Größen von Linked-Clone-Festplatten, wenn Sie einen Pool bearbeiten oder Replikate in einem separaten Datenspeicher ablegen.

Tabelle 5-10. Formeln zur Größenberechnung von Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

Datentyp	Ausgewählter freier Speicherplatz (GB)	Mind. empfohlen (GB)	50% Auslastung (GB)	Max. empfohlen (GB)
Betriebssystemfestplatten	Freier Speicherplatz in den ausgewählten Datenspeichern	Anzahl der VMs * (2 * Arbeitsspeicher der VM)	Anzahl der VMs * (50% der Replikatfestplatte + Arbeitsspeicher der VM)	Anzahl der VMs * (100% der Replikatfestplatte + Arbeitsspeicher der VM)
Persistent disks (Persistente Festplatten)	Freier Speicherplatz in den ausgewählten Datenspeichern	Anzahl der VMs * 20% der persistenten Festplatte	Anzahl der VMs * 50% der persistenten Festplatte	Anzahl der VMs * 100% der persistenten Festplatte

Beispiel einer geschätzte Speichergröße beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

In diesem Beispiel wird die übergeordnete virtuelle Maschine mit einem Arbeitsspeicher von 1 GB konfiguriert. Die Festplatte der übergeordneten virtuellen Maschine ist 10 GB groß. Es wird ein Linked-Clone-Pool mit 10 Desktops erstellt. Die Größe der persistenten Festplatten wird auf 2048 MB festgelegt.

Die Betriebssystemfestplatten werden in einem Datenspeicher konfiguriert, der derzeit über 184,23 GB freien Speicherplatz verfügt. Die persistenten Festplatten werden in einem anderen Datenspeicher mit 28,56 GB freiem Speicherplatz konfiguriert.

Tabelle 5-11 zeigt, wie mithilfe der Formeln zur Größenberechnung die geschätzten Speicheranforderungen für den beispielhaften Linked-Clone-Pool ermittelt werden.

Tabelle 5-11. Beispiel einer geschätzte Speichergröße für Linked-Clone-Festplatten beim Bearbeiten von Pools oder zum Speichern von Replikaten in separaten Datenspeichern

Datentyp	Ausgewählter freier Speicherplatz (GB)	Mind. empfohlen (GB)	50% Auslastung (GB)	Max. empfohlen (GB)
Betriebssystemfestplatten	184.23	10 * (2 * 1 GB) = 20.00	10 * (50% von 10 GB + 1 GB) = 60,00	10 * (100% von 10 GB + 1 GB) = 110,00
Persistent disks (Persistente Festplatten)	28.56	10 * (20% von 2 GB) = 4,00	10 * (50% von 2 GB) = 10,00	10 * (100% von 2 GB) = 20,00

Festlegen des Werts für die Speichermehrfachvergabe für Linked-Clone-Desktops

Mithilfe der Funktion für die Speichermehrfachvergabe kann gesteuert werden, wie viele Linked-Clone-Desktops View Manager in einem Datenspeicher erstellt. Über diese Funktion können Sie verknüpfte Klone erstellen, deren logische Größe insgesamt den physischen Speichergrenzwert des Datenspeichers überschreitet.

Diese Funktion kann nur mit Linked-Clone-Pools verwendet werden.

Der Grad der Speichermehrfachvergabe gibt an, um wie viel größer die Speichermenge gegenüber der physischen Größe des Datenspeichers ist, den die Klone verwenden würden, wenn es sich um vollständige virtuelle Maschinen handeln würde. Weitere Informationen finden Sie unter „Speichermehrfachvergabe für Linked-Clone-Desktops“, auf Seite 108.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Wenn Sie einen neuen Desktop-Pool erstellen oder einen vorhandenen Pool bearbeiten, navigieren Sie zur Seite Select Datastores (Datenspeicher auswählen).

Option	Aktion
Neuer Desktop-Pool	a Klicken Sie auf **[Add (Hinzufügen)]** . b Fahren Sie im Assistenten zum Hinzufügen von Pools fort, bis die Seite Select Datastores (Datenspeicher auswählen) angezeigt wird.
Vorhandener Desktop-Pool	a Wählen Sie den Linked-Clone-Pool aus und klicken Sie auf **[Edit (Bearbeiten)]** . b Klicken Sie auf die Registerkarte **[vCenter Settings (vCenter-Einstellungen)]** .

3 Wählen Sie auf der Seite Select Datastores (Datenspeicher auswählen) den Grad der Speichermehrfachvergabe aus.

Option	Beschreibung
–	Es findet keine Speichermehrfachvergabe statt.
Conservative (Konservativ)	4-fache Größe des Datenspeichers. Dies ist der Standardwert.
Moderate (Mittel)	7-fache Größe des Datenspeichers.
Aggressive (Aggressiv)	15-fache Größe des Datenspeichers.

4 Klicken Sie auf **[Done (Fertig)]** .

5 Klicken Sie auf **[Finish (Fertig stellen)]** .

Speichermehrfachvergabe für Linked-Clone-Desktops

Mithilfe der Funktion zur Speichermehrfachvergabe können Sie die Speicherkosten reduzieren, indem Sie mehr Linked-Clone-Desktops in einem Datenspeicher platzieren, als dies bei vollständigen virtuellen Maschinen-Desktops möglich ist. Die verknüpften Klone können das Mehrfache der physischen Datenspeicherkapazität als logischen Speicherplatz verwenden.

Mit dieser Funktion können Sie eine Speicherebene wählen, bei der eine Speichermehrfachvergabe für die Kapazität des Datenspeichers möglich ist. Zudem wird die Anzahl an verknüpften Klonen eingeschränkt, die View Manager erstellt. Sie können einerseits die Vergeudung von Speicherkapazität durch eine zu konservative Bereitstellung und andererseits das Risiko verhindern, dass der Speicherplatz für die verknüpften Klone knapp wird und die zugehörigen Desktop-Anwendungen fehlschlagen.

Beispielsweise können Sie maximal zehn vollständige virtuelle Maschinen in einem Datenspeicher mit 100 GB erstellen, wenn die Größe jeder virtuellen Maschine 10 GB beträgt. Wenn Sie aus einer übergeordneten virtuellen Maschine mit 10 GB verknüpfte Klone erstellen, weist jeder Klon einen Bruchteil dieser Größe auf.

Wenn Sie einen konservativen Wert für die Speichermehrfachvergabe festlegen, können die Klone das Vierfache der physischen Datenspeichergröße verwenden. Für die Größe der einzelnen Klone wird von der Größe der übergeordneten virtuellen Maschine ausgegangen. Bei einem Datenspeicher mit 100 GB und einer übergeordneten virtuellen Maschine mit 10 GB stellt View Manager etwa 40 verknüpfte Klone bereit. View Manager stellt auch dann keine größere Anzahl an Klonen bereit, wenn der Datenspeicher über freien Speicherplatz verfügt. Diese Beschränkung bietet einen Puffer für das Wachstum vorhandener Klone.

Tabelle 5-12 zeigt die möglichen Werte für die Speichermehrfachvergabe.

Tabelle 5-12. Grad der Speichermehrfachvergabe

Option	Grad der Speichermehrfachvergabe
–	Es findet keine Speichermehrfachvergabe statt.
Conservative (Konservativ)	4-fache Größe des Datenspeichers. Dies ist der Standardwert.
Moderate (Mittel)	7-fache Größe des Datenspeichers.
Aggressive (Aggressiv)	15-fache Größe des Datenspeichers.

Die Werte für die Speichermehrfachvergabe bieten eine allgemeine Richtlinie zum Bestimmen der Speicherkapazität. Um den idealen Wert zu ermitteln, überwachen Sie das Wachstum der verknüpften Klone in Ihrer Umgebung.

Legen Sie einen sehr hohen Wert fest, wenn die Betriebssystemfestplatten die mögliche Maximalgröße nie erreichen werden. Bei einem hohen Wert für die Speichermehrfachvergabe muss die Umgebung sorgfältig überwacht werden. Um sicherzustellen, dass der Speicherplatz für die verknüpften Klone nicht knapp wird, können Sie den Desktop-Pool regelmäßig aktualisieren oder neu verteilen und die Betriebssystemdaten der verknüpften Klone auf die ursprüngliche Größe reduzieren.

Beispielsweise ist ein hoher Wert für die Speichermehrfachvergabe für einen Desktop-Pool mit dynamischer Zuweisung sinnvoll, für dessen Desktops nach der Abmeldung ein Lösch- oder Aktualisierungsvorgang festgelegt ist.

Sie können für verschiedene Datenspeichertypen unterschiedliche Werte für die Speichermehrfachvergabe festlegen, um den unterschiedlichen Durchsatzleistungen in den einzelnen Datenspeichern Rechnung zu tragen. Für einen NAS-Datenspeicher kann beispielsweise eine andere Einstellung gewählt werden als für einen SAN-Datenspeicher.

Speichern von View Composer-Replikaten und verknüpften Klonen in separaten Datenspeichern

Sie können View Composer-Replikate und verknüpfte Klone in separaten Datenspeichern mit unterschiedlichen Leistungsmerkmalen ablegen. Diese flexible Konfiguration kann intensive Vorgänge wie die gleichzeitige Bereitstellung zahlreicher verknüpfter Klone oder die Ausführung von Antivirenscans beschleunigen.

Beispielsweise können Sie die virtuellen Replikatmaschinen in einem auf einer Solid-State-Disk basierenden Datenspeicher speichern. Solid-State-Disks besitzen eine niedrige Speicherkapazität und eine hohe Leseleistung, in der Regel mit Unterstützung für 20.000 E/A-Vorgänge pro Sekunde (IOPS). View Composer erstellt nur ein Replikat für jeden View Composer-Basis-Image-Snapshot in jedem ESX-Cluster, sodass Replikate nicht viel Speicherplatz in Anspruch nehmen. Eine Solid-State-Disk kann die Geschwindigkeit verbessern, in der ESX die Betriebssystemfestplatte eines Replikats liest, wenn eine Aufgabe gleichzeitig auf vielen verknüpften Klonen ausgeführt wird.

Sie können verknüpfte Klone auf herkömmlichen, auf drehenden Medien basierenden Datenspeichern speichern. Diese Festplatten bieten eine geringere Leistung und unterstützen in der Regel 200 E/A-Vorgänge pro Sekunde. Sie sind kostengünstig und bieten eine hohe Speicherkapazität, wodurch sie zur Speicherung der zahlreichen verknüpften Klone in einem großen Pool geeignet sind. ESX muss keine intensiven, gleichzeitigen Lesevorgänge für einen verknüpften Klon ausführen.

Indem Sie Replikate und verknüpfte Klone auf diese Weise konfigurieren, können Sie die Auswirkungen von E/A-Überlastungen bei gleichzeitiger Erstellung vieler verknüpfter Klone reduzieren. Wenn Sie beispielsweise einen Pool mit dynamischer Zuweisung mit einer Richtlinie zum Löschen von Desktops bei Abmeldung bereitstellen und die Benutzer gleichzeitig mit der Arbeit beginnen, muss View Manager für alle gleichzeitig neue Desktops bereitstellen.

Wichtig Diese Funktion ist auf bestimmte Speicherkonfigurationen ausgelegt, die von Herstellern mit Hochleistungsfestplatten-Lösungen bereitgestellt werden. Speichern Sie Replikate nicht in einem separaten Datenspeicher, wenn Ihre Speicherhardware keine hohe Leseleistung unterstützt.

Sie müssen bestimmte Anforderungen einhalten, wenn Sie das Replikat und verknüpfte Klone in einem Pool auf separaten Datenspeichern speichern:

- Sie können nur einen separaten Replikatdatenspeicher für einen Pool angeben.
- Wenn ein Replikatdatenspeicher gemeinsam genutzt wird, muss er von allen ESX-Hosts im Cluster aus zugänglich sein.
- Werden die Linked-Clone-Datenspeicher gemeinsam verwendet, muss der Replikatdatenspeicher freigegeben werden. Replikate können nur dann in einem lokalen Datenspeicher abgelegt werden, wenn Sie alle verknüpften Klone in lokalen Datenspeichern auf demselben ESX-Host konfigurieren.

Überlegungen zur Verfügbarkeit beim Speichern von Replikaten in einem separaten oder in gemeinsam genutzten Datenspeichern

Sie können View Composer-Replikate in einem separaten Datenspeicher oder in denselben Datenspeichern wie virtuelle Linked-Clone-Maschinen speichern. Diese Konfigurationen wirken sich unterschiedlich auf die Verfügbarkeit des Pools aus.

Wenn Sie Replikate in denselben Datenspeichern wie verknüpfte Klone ablegen, erstellt View Composer zur besseren Verfügbarkeit in jedem Datenspeicher ein separates Replikat. Steht ein Datenspeicher nicht mehr zur Verfügung, sind nur die verknüpften Klone im jeweiligen Datenspeicher betroffen. Verknüpfte Klone in anderen Datenspeichern werden weiterhin ausgeführt.

Wenn Sie Replikate in einem separaten Datenspeicher ablegen, werden alle verknüpften Klone im Pool mit den Replikaten in dem jeweiligen Datenspeicher gekoppelt. Fällt der Datenspeicher aus, steht der gesamte Pool nicht länger zur Verfügung.

Um die Verfügbarkeit von Linked-Clone-Desktops zu verbessern, können Sie für den Datenspeicher, in dem Sie die Replikate speichern, eine Hochverfügbarkeitslösung konfigurieren.

Datenfestplatten von Linked-Clone-Desktops

View Composer erstellt mehrere Datenfestplatten zum Speichern der Komponenten eines Linked-Clone-Desktops.

Betriebssystemfestplatte

View Composer erstellt eine Betriebssystemfestplatte für jeden verknüpften Klon. Auf dieser Festplatte werden die Systemdaten gespeichert, die der Klon benötigt, um mit dem Basis-Image verknüpft zu bleiben und als eindeutig identifizierbarer Desktop zu fungieren.

QuickPrep-Konfigurationsdatenfestplatte

View Composer erstellt mit der Betriebssystemfestplatte eine zweite Festplatte. Auf der zweiten Festplatte werden QuickPrep-Konfigurationsdaten und andere betriebssystembezogene Daten gespeichert, die während Aktualisierungen und Neuzusammenstellungen beibehalten werden müssen. Diese Festplatte ist klein und umfasst in der Regel etwa 20 MB. Diese Festplatte wird erstellt, wenn Sie mithilfe von QuickPrep oder Sysprep den Desktop anpassen.

Wenn Sie separate persistente View Composer-Festplatten zum Speichern von Benutzerprofilen konfigurieren, werden jedem verknüpften Klon drei Festplatten zugewiesen: die Betriebssystemfestplatte, die zweite Desktop-Festplatte und die persistente View Composer-Festplatte.

Die zweite Desktop-Festplatte wird in demselben Datenspeicher wie die Betriebssystemfestplatte gespeichert. Diese Festplatte kann nicht konfiguriert werden.

Persistente View Composer-Festplatte

In einem Pool mit dedizierter Zuweisung können Sie separate persistente View Composer-Festplatten zum Speichern von Windows-Benutzerprofildaten konfigurieren. Diese Festplatte ist optional.

Separate persistente Festplatten ermöglichen Ihnen das Beibehalten von Benutzerdaten und -einstellungen. View Composer-Aktualisierungen, -Neuzusammenstellungen und Neuverteilungen wirken sich nicht auf persistente Festplatten aus. Sie können eine persistente Festplatte von einem verknüpften Klon trennen und mit einem anderen verknüpften Klon verknüpfen.

Wenn Sie keine separaten persistenten Festplatten konfigurieren, wird das Windows-Profil auf der Betriebssystemfestplatte gespeichert. Benutzerdaten und -einstellungen werden während Aktualisierungen, Neuzusammenstellungen und Neuverteilungen entfernt.

Sie können persistente Festplatten in demselben Datenspeicher wie die Betriebssystemfestplatte oder in einem anderen Datenspeicher ablegen.

Festplatte für löschbare Daten

Bei der Erstellung eines Linked-Clone-Pools können Sie eine separate, nicht persistente Festplatte zum Speichern der Auslagerungs- und temporären Dateien des Gastbetriebssystems konfigurieren, die bei Benutzersitzungen generiert werden. Die Festplattengröße muss in Megabyte angegeben werden.

Diese Festplatte ist optional.

Beim Ausschalten eines verknüpften Klons ersetzt View Manager die Festplatte mit löschbaren Daten durch eine Kopie der ursprünglichen Festplatte, die View Composer mit dem Linked-Clone-Pool erstellt hat. Verknüpfte Klone können an Größe zunehmen, wenn Benutzer mit ihren Desktops interagieren. Durch Verwendung von Festplatten mit löschbaren Daten kann Speicherplatz eingespart werden, indem das Wachstum verknüpfter Klone verlangsamt wird.

Die Festplatte für löschbare Daten wird in demselben Datenspeicher wie die Betriebssystemfestplatte gespeichert.

Manuelle Desktop-Pools

Zum Erstellen eines manuellen Desktop-Pools stellt View Manager Desktops von vorhandenen Desktop-Quellen bereit. Für jeden Desktop im Pool wählen Sie eine separate Desktop-Quelle bereit, um den Clients View-Zugriff zu ermöglichen.

View Manager kann mehrere Arten von Desktop-Quellen in manuellen Pools verwenden:

- Mit vCenter Server verwaltete virtuelle Maschinen
- Auf VMware Server oder einer anderen Virtualisierungsplattform ausgeführte virtuelle Maschinen
- Physische Computer
- HP Blade-PCs

Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools

Bei der Erstellung eines manuellen Desktop-Pools fordert der View Administrator-Assistent zum Hinzufügen von Pools Sie zum Konfigurieren bestimmter Optionen auf. Mithilfe dieses Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie den Pool erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie bei Ausführung des Assistenten zum Hinzufügen von Pools angeben möchten.

Hinweis In einem manuellen Pool müssen Sie jede Desktop-Quelle so vorbereiten, dass sie View-Desktop-Zugriff bereitstellt. View Agent muss auf jeder Desktop-Quelle installiert sein und ausgeführt werden.

Tabelle 5-13. Arbeitsblatt: Konfigurationsoptionen zum Erstellen eines manuellen Desktop-Pools

Option	Beschreibung	Wert
User assignment (Benutzerzuweisung)	Wählen Sie die Art der Benutzerzuweisung: ■ In einem Pool mit dedizierter Zuweisung wird jeder Benutzer einem Desktop zugewiesen. Benutzer erhalten bei jeder Anmeldung denselben Desktop. ■ In einem Pool mit dynamischer Zuweisung erhalten die Benutzer bei jeder Anmeldung einen anderen Desktop. Weitere Informationen finden Sie unter „Benutzerzuweisung in Desktop-Pools“, auf Seite 119.	
Desktop Sources (Desktop-Quellen)	Die virtuellen Maschinen oder physischen Computer, die Sie als View-Desktops im Pool verwenden möchten. 1 Entscheiden Sie, welchen Typ der Desktop-Quelle Sie verwenden möchten. Sie können entweder virtuelle Maschinen einsetzen, die von vCenter Server verwaltet werden, oder nicht verwaltete virtuelle Maschinen, physische Computer und Blade-PCs. 2 Bereiten Sie eine Liste mit virtuellen vCenter Server-Maschinen oder nicht verwalteten virtuellen Maschinen, physischen Computern und Blade-PCs vor, die Sie in den Pool aufnehmen möchten. Um PCoIP mit Desktop-Quellen zu verwenden, bei denen es sich um nicht verwaltete virtuelle Maschinen, physische Computer oder Blade-PCs handelt, müssen Sie Teradici-Hardware einsetzen.	
vCenter Server	Die vCenter Server-Instanz, welche die Desktops verwaltet. Diese Option wird nur angezeigt, wenn es sich bei den Desktop-Quellen um virtuelle Maschinen handelt, die von vCenter Server verwaltet werden.	
Pool ID (Pool-ID)	Der Pool-Name, der Benutzern bei der Anmeldung angezeigt wird und der den Pool in View Administrator identifiziert. Wenn mehrere vCenter Server-Instanzen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere vCenter Server-Instanz dieselbe Pool-ID verwendet.	
Pool Settings (Pool-Einstellungen)	Einstellungen, die den Desktop-Status, den Betriebsstatus bei Nichtnutzung einer virtuellen Maschine, das Anzeigeprotokoll, die Adobe Flash-Qualität usw. festlegen. Weitere Informationen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126. Eine Liste der Einstellungen für manuelle Pools finden Sie unter „Desktop-Einstellungen für manuelle Pools“, auf Seite 115.	

Erstellen eines manuellen Desktop-Pools

Sie können einen manuellen Desktop-Pool erstellen, der Desktops von vorhanden virtuellen Maschinen, physischen Computern und HP Blade-PCs bereitstellt. Sie müssen die Desktop-Quellen auswählen, aus denen die View-Desktops im Pool bestehen.

Für manuelle Pools mit Desktops, die über vCenter Server verwaltet werden, schaltet View Manager einen Reserve-Desktop ein, damit die Benutzer sich verbinden können. Der Reserve-Desktop wird unabhängig davon eingeschaltet, welche Betriebsrichtlinie in Kraft ist.

Voraussetzungen

- Bereiten Sie die Desktop-Quellen für das Bereitstellen von Zugriff auf einen View-Desktop vor. In einem manuellen Pool müssen Sie jede Desktop-Quelle einzeln vorbereiten. View Agent muss auf jeder Desktop-Quelle installiert sein und ausgeführt werden.

  Informationen zum Vorbereiten einer von vCenter Server verwalteten virtuellen Maschine finden Sie unter Kapitel 4, „Erstellen und Vorbereiten virtueller Maschinen“, auf Seite 51.

  Informationen zum Vorbereiten nicht verwalteter virtueller Maschinen, physischer Computer oder Blade-PCs finden Sie unter Kapitel 3, „Vorbereiten nicht verwalteter Desktop-Quellen“, auf Seite 47.

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des Pools bereitstellen müssen. Siehe „Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools“, auf Seite 111.

- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe „Desktop- und Pool-Einstellungen“, auf Seite 126.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Klicken Sie auf **[Add (Hinzufügen)]** .

3 Wählen Sie **[Manual Pool (Manueller Pool)]** .

4 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

  Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

In View Administrator können Sie die Desktops so anzeigen, wie sie dem Pool hinzugefügt werden. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Desktops]** .

Weiter

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139.

Erstellen eines manuellen Pools mit einem Desktop

Sie können einen Pool mit einem einzigen Desktop erstellen, wenn Benutzer einen eindeutigen dedizierten Desktop benötigen oder wenn mehrere Benutzer zu unterschiedlichen Zeiten auf eine kostspielige Anwendung mit einer einzelnen Hostlizenz zugreifen müssen.

Sie können einen einzelnen View-Desktop in einem eigenen Pool bereitstellen, indem Sie einen manuellen Desktop-Pool erstellen und eine einzige Desktop-Quelle auswählen.

Um einen physischen Computer zu simulieren, der von mehreren Benutzern gemeinsam verwendet werden kann, geben Sie eine dynamische Zuweisung für die Benutzer an, die zum Zugriff auf den Pool berechtigt sind.

Unabhängig davon, ob Sie einen Pool mit einem einzelnen Desktop mit einer dynamischen oder dedizierten Zuweisung konfigurieren, werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Die virtuelle Maschine wird eingeschaltet, wenn ein Benutzer den Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet.

Wenn Sie die Richtlinie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** konfigurieren, bleibt die virtuelle Maschine immer eingeschaltet. Wenn der Benutzer die virtuelle Maschine herunterfährt, wird sie sofort neu gestartet.

Voraussetzungen

- Bereiten Sie die Desktop-Quelle für das Bereitstellen von Zugriff auf einen View-Desktop vor. View Agent muss auf der Desktop-Quelle installiert sein und ausgeführt werden.

  Informationen zum Vorbereiten einer von vCenter Server verwalteten virtuellen Maschine finden Sie unter Kapitel 4, „Erstellen und Vorbereiten virtueller Maschinen“, auf Seite 51.

  Informationen zum Vorbereiten einer nicht verwalteten virtuellen Maschine, eines physischen Computers oder Blade-PCs finden Sie unter Kapitel 3, „Vorbereiten nicht verwalteter Desktop-Quellen“, auf Seite 47.

- Sammeln Sie die Konfigurationsinformationen, die Sie zum Erstellen des manuellen Pools bereitstellen müssen. Siehe „Arbeitsblatt zum Erstellen eines manuellen Desktop-Pools“, auf Seite 111.

- Entscheiden Sie, wie die Betriebseinstellungen, das Anzeigeprotokoll, die Adobe Flash-Qualität und andere Einstellungen konfiguriert werden sollen. Siehe „Desktop- und Pool-Einstellungen“, auf Seite 126.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Klicken Sie auf **[Add (Hinzufügen)]** .

3 Wählen Sie **[Manual Pool (Manueller Pool)]** .

4 Wählen Sie die Art der Benutzerzuweisung.

Option	Beschreibung
Dedizierte Zuweisung	Der Desktop ist einem Benutzer zugewiesen. Nur dieser Benutzer kann sich am Desktop anmelden.
Dynamische Zuweisung	Der Desktop wird von allen Benutzern gemeinsam genutzt, die über Berechtigungen für den Pool verfügen. Jeder berechtigte Benutzer kann sich am Desktop anmelden, sofern zurzeit kein anderer Benutzer angemeldet ist.

5 Wählen Sie auf der Seite **[Add vCenter Virtual Machines (Virtuelle vCenter-Maschinen hinzufügen)]** bzw. **[Add Machines (Maschinen hinzufügen)]** die Desktop-Quelle für Ihren Desktop aus.

6 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

  Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt zusammengetragen haben. Sie können jederzeit auf eine beliebige Assistentenseite zurückwechseln, die Sie bereits ausgefüllt haben, indem Sie im Navigationsbereich auf den Seitennamen klicken.

In View Administrator können Sie den Desktop so anzeigen, wie er erstellt wird. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Desktops]** .

Weiter

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139.

Desktop-Einstellungen für manuelle Pools

Beim Konfigurieren manueller Pools müssen Sie Desktop- und Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen manueller Pools.

Tabelle 5-14 werden die Einstellungen aufgeführt, die für mit diesen Eigenschaften konfigurierte manuelle Desktop-Pools gelten:

- Dedizierte Benutzerzuweisungen
- Dynamische Benutzerzuweisungen
- Verwaltete Desktop-Quellen (virtuelle vCenter Server-Maschinen)
- Nicht verwaltete Desktop-Quellen

Diese Einstellungen gelten auch für einen manuellen Pool mit einem einzigen Desktop.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126.

Tabelle 5-14. Einstellungen für manuelle Desktop-Pools

Einstellung	Manueller verwalteter Pool, dedizierte Zuweisung	Manueller verwalteter Pool, dynamische Zuweisung	Manueller nicht verwalteter Pool, dedizierte Zuweisung	Manueller nicht verwalteter Pool, dynamische Zuweisung
State (Status)	Ja.	Ja.	Ja.	Ja.
Connection Server Restrictions (Einschränkungen für Connection Server)	Ja.	Ja.	Ja.	Ja.
Betriebsrichtlinie für Remote-Desktops	Ja.	Ja.		
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	Ja.	Ja.	Ja.	Ja.
Allow users to reset their desktop (Benutzern das Zurücksetzen ihrer Desktops gestatten)	Ja.	Ja.		
Allow multiple sessions per user (Mehrere Sitzungen pro Benutzer zulassen)		Ja.		Ja.

Tabelle 5-14. Einstellungen für manuelle Desktop-Pools (Fortsetzung)

Einstellung	Manueller verwalteter Pool, dedizierte Zuweisung	Manueller verwalteter Pool, dynamische Zuweisung	Manueller nicht verwalteter Pool, dedizierte Zuweisung	Manueller nicht verwalteter Pool, dynamische Zuweisung
Default display protocol (Standardanzeigeprotokoll)	Ja.	Ja.	Ja. Um PCoIP mit einer Desktop-Quelle zu verwenden, die nicht von vCenter Server verwaltet wird, müssen Sie Teradici-Hardware auf der Desktop-Quelle installieren.	Ja. Um PCoIP mit einer Desktop-Quelle zu verwenden, die nicht von vCenter Server verwaltet wird, müssen Sie Teradici-Hardware auf der Desktop-Quelle installieren.
Allow users to choose a protocol (Benutzern die Wahl des Protokolls erlauben)	Ja.	Ja.	Ja.	Ja.
Windows 7-3D-Rendering	Ja.	Ja.		
Max number of monitors (Maximale Anzahl an Monitoren)	Ja.	Ja.		
Max resolution of any one monitor (Max. Auflösung eines Monitors)	Ja.	Ja.		
Adobe Flash quality (Adobe Flash-Qualität)	Ja.	Ja.	Ja.	Ja.
Adobe Flash throttling (Adobe Flash-Drosselung)	Ja.	Ja.	Ja.	Ja.

Microsoft-Terminaldienste-Pools

Sie können Microsoft-Terminalserver einsetzen, um Terminaldienste-Sitzungen als Desktops für View-Clients bereitzustellen. View Manager verwaltet Terminaldienste-Sitzungen auf dieselbe Weise wie andere View-Desktops.

Ein Terminaldienste-Pool kann mehrere Desktop-Quellen enthalten, die von einem oder mehreren Terminalservern bedient werden. Eine Terminalserver-Desktop-Quelle kann mehrere View-Desktops bereitstellen.

View Manager ermöglicht einen Lastausgleich zwischen den Terminalservern in einem Pool, indem Verbindungsanfragen an den Terminalserver geleitet werden, auf dem die geringste Anzahl aktiver Sitzungen vorliegt.

Sie berechtigen einen gesamten Terminaldienste-Pool für Benutzer oder Benutzergruppen.

Servergespeicherte Profile sollten eingesetzt werden, um Benutzereinstellungen und Daten auf den Desktop zu übertragen, auf den der Benutzer derzeit zugreift.

HINWEIS Terminaldienste-Pools unterstützen nur das RDP-Anzeigeprotokoll.

Erstellen eines Microsoft-Terminaldienste-Pools

Sie können einen Microsoft-Terminaldienste-Pool erstellen, der Desktops von Terminalserver-Desktop-Quellen bereitstellt. Sie müssen die Desktop-Quellen auswählen, aus denen die View-Desktops im Pool bestehen.

Voraussetzungen

- Bereiten Sie die Terminalserver-Desktop-Quellen für das Bereitstellen von Zugriff auf einen View-Desktop vor. View Agent muss auf jeder Desktop-Quelle installiert sein und ausgeführt werden. Siehe Kapitel 3, „Vorbereiten nicht verwalteter Desktop-Quellen“, auf Seite 47.
- Erstellen Sie eine Liste der Terminalserver-Desktop-Quellen, die Sie in den Pool aufnehmen möchten.
- Entscheiden Sie, wie die Desktop-Einstellungen konfiguriert werden sollen. Siehe „Desktop-Einstellungen für Microsoft-Terminaldienste-Pools“, auf Seite 117. Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126.
- Stellen Sie eine Pool-ID bereit, die Benutzern bei der Anmeldung angezeigt wird und die den Pool in View Administrator identifiziert. Wenn mehrere vCenter Server-Instanzen in Ihrer Umgebung ausgeführt werden, stellen Sie sicher, dass keine weitere vCenter Server-Instanz dieselbe Pool-ID verwendet.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Klicken Sie auf **[Add (Hinzufügen)]** .

3 Wählen Sie **[Microsoft Terminal Services Desktop Pool (Microsoft-Terminaldienste-Desktop-Pool)]** .

4 Folgen Sie den Anweisungen des Assistenten, um den Pool zu erstellen.

Verwenden Sie die im Arbeitsblatt erfassten Konfigurationsinformationen. Sie können direkt zu einer beliebigen Seite des Assistenten zurückgehen, indem Sie im Navigationsbereich auf den Seitennamen klicken.

In View Administrator können Sie die Desktops so anzeigen, wie sie dem Pool hinzugefügt werden. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Desktops]** .

Weiter

Erteilen Sie Benutzern die Berechtigung für den Zugriff auf den Pool. Siehe „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139.

Desktop-Einstellungen für Microsoft-Terminaldienste-Pools

Beim Konfigurieren von Microsoft-Terminaldienste-Pools müssen Sie Desktop- und Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen von Terminaldienste-Pools.

Tabelle 5-15 werden die Einstellungen aufgeführt, die für Terminaldienste-Pools gelten.

Beschreibungen der einzelnen Desktop-Einstellungen finden Sie unter „Desktop- und Pool-Einstellungen“, auf Seite 126.

Tabelle 5-15. Einstellungen für Terminaldienste-Pools

Einstellung	Microsoft-Terminaldienste-Pool
State (Status)	Ja.
Connection Server Restrictions (Einschränkungen für Connection Server)	Ja.
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	Ja.

Tabelle 5-15. Einstellungen für Terminaldienste-Pools (Fortsetzung)

Einstellung	Microsoft-Terminaldienste-Pool
Default display protocol (Standardanzeigeprotokoll)	Für Terminaldienste-Pools wird nur das RDP-Anzeigeprotokoll unterstützt.
Adobe Flash quality (Adobe Flash-Qualität)	Ja.
Adobe Flash throttling (Adobe Flash-Drosselung)	Ja.

Konfigurieren der Adobe Flash-Drosselung in Internet Explorer für Terminaldienste-Sitzungen

Um sicherzustellen, dass die Adobe Flash-Drosselung in Internet Explorer für Terminaldienste-Sitzungen funktioniert, müssen die Benutzer Browsererweiterungen von Drittanbietern aktivieren.

Vorgehensweise

1 Starten Sie View Client und melden Sie sich an einem Benutzer-Desktop an.

2 Klicken Sie in Internet Explorer auf **[Tools (Extras)]** > **[Internet Options (Internetoptionen)]** .

3 Klicken Sie auf die Registerkarte **[Advanced (Erweitert)]** , wählen Sie **[Enable third-party browser extensions (Browsererweiterungen von Drittanbietern aktivieren)]** und klicken Sie auf **[OK]** .

4 Starten Sie Internet Explorer neu.

Bereitstellen von Desktop-Pools

Bei der Erstellung eines Desktop-Pools legen Sie mithilfe von Konfigurationsoptionen fest, wie der Pool verwaltet wird und wie Benutzer mit den Desktops interagieren.

- Benutzerzuweisung in Desktop-Pools auf Seite 119

  Sie können einen Desktop-Pool so konfigurieren, dass die Desktops im Pool den Benutzern dediziert oder dynamisch zugewiesen werden. Sie müssen eine Benutzerzuweisung für automatisierte Pools, die vollständige virtuelle Maschinen enthalten, für automatisierte Linked-Clone-Pools und für manuelle Pools auswählen.

- Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters auf Seite 119

  Sie können die Desktops in einem automatisierten Pool bereitstellen, indem Sie manuell eine Liste von Desktop-Namen angeben oder ein Benennungsmuster sowie die Anzahl der Desktops festlegen, die im Pool enthalten sein sollen. Diese beiden Ansätze bieten unterschiedliche Vorteile.

- Manuelles Anpassen von Desktops auf Seite 125

  Nach der Erstellung eines automatisierten Pools können Sie bestimmte Desktops anpassen, ohne den Besitz neu zuzuweisen. Durch das Starten der Desktops im Wartungsmodus können Sie die Desktops ändern und testen, bevor Sie sie den zugewiesenen Benutzern freigeben oder allen berechtigten Benutzern im Pool zur Verfügung stellen.

- Desktop- und Pool-Einstellungen auf Seite 126

  Bei der Konfiguration von automatisierten Pools mit vollständigen virtuellen Maschinen, Linked-Clone-Desktop-Pools, manuellen Desktop-Pools und Microsoft-Terminaldienste-Pools müssen Sie Desktop- und Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen von Desktop-Pools.

- Konfigurieren von 3D-Rendern auf Windows 7-Desktops auf Seite 131

  Wenn Sie einen Windows 7-Desktop-Pool erstellen, können Sie das 3D-Grafikrendering für Ihre Desktops konfigurieren. Wenn Sie diese Desktop-Einstellung auswählen, können die Benutzer die Vorteile von Grafikverbesserungen nutzen, die durch Anwendungen wie AERO, Microsoft Office 2010 und Google Earth bereitgestellt werden.

- Verhindern vom Zugriff auf View-Desktops durch RDP auf Seite 131

  In bestimmten View-Umgebungen ist die Verhinderung eines Zugriffs auf View-Desktops durch das RDP-Anzeigeprotokoll eine Priorität. Sie können die Benutzer und Administratoren beim Zugriff auf View-Desktops von der RDP-Verwendung abhalten, indem Sie die Pool-Einstellungen und die Gruppenrichtlinieneinstellungen konfigurieren.

Benutzerzuweisung in Desktop-Pools

Sie können einen Desktop-Pool so konfigurieren, dass die Desktops im Pool den Benutzern dediziert oder dynamisch zugewiesen werden. Sie müssen eine Benutzerzuweisung für automatisierte Pools, die vollständige virtuelle Maschinen enthalten, für automatisierte Linked-Clone-Pools und für manuelle Pools auswählen.

Bei einer dedizierten Zuweisung weist View Manager jedem berechtigten Benutzer einen Desktop im Pool zu. Wenn ein Benutzer sich mit einem Pool verbindet, meldet sich der Benutzer immer an demselben Desktop an. Die Benutzereinstellungen und -daten werden zwischen den Sitzungen gespeichert. Kein anderer Benutzer im Pool kann auf den Desktop zugreifen.

Bei einer dynamischen Zuweisung weist View Manager Desktops im Pool den berechtigten Benutzern dynamisch zu. Benutzer verbinden sich bei jeder Anmeldung mit einem anderen Desktop. Wenn der Benutzer sich abmeldet, wird der Desktop wieder dem Pool zurückgegeben.

Sie können Desktops mit dynamischer Zuweisung so konfigurieren, dass sie bei der Benutzerabmeldung gelöscht werden. Durch den automatischen Löschvorgang können Sie immer nur die benötigte Anzahl virtueller Maschinen beibehalten. Der automatische Löschvorgang ist nur in automatisierten Pools möglich, die Sie mit einem Desktop-Benennungsmuster und einer Gesamtzahl an Desktops bereitstellen.

Durch Desktops mit dynamischer Zuweisung können Sie die Kosten für die Softwarelizenzierung senken.

Manuelles Benennen von Desktops oder Bereitstellen eines Benennungsmusters

Sie können die Desktops in einem automatisierten Pool bereitstellen, indem Sie manuell eine Liste von Desktop-Namen angeben oder ein Benennungsmuster sowie die Anzahl der Desktops festlegen, die im Pool enthalten sein sollen. Diese beiden Ansätze bieten unterschiedliche Vorteile.

Wenn Sie Desktops durch Angabe einer Liste benennen, können Sie das Namensschema Ihres Unternehmens verwenden und jeden Desktop-Namen mit einem Benutzer verknüpfen.

Wenn Sie ein Benennungsmuster bereitstellen, kann View Manager Desktops dynamisch nach Bedarf der Benutzer erstellen und zuweisen.

Sie müssen eine dieser Benennungsmethoden zur Bereitstellung automatisierter Pools anwenden, die vollständige virtuelle Maschinen oder verknüpfte Klone enthalten.

In Tabelle 5-16 werden die beiden Benennungsmethoden verglichen. Ferner wird gezeigt, wie die jeweilige Methode sich auf die Erstellung und Verwaltung eines Desktop-Pools auswirkt.

Tabelle 5-16. Manuelles Benennen von Desktops oder Bereitstellen eines Desktop-Benennungsmusters

Funktion	Bereitstellen eines Desktop-Benennungsmusters	Manuelles Benennen von Desktops
Desktop-Namen	View Manager generiert Desktop-Namen. Sie stellen ein Benennungsmuster bereit. View Manager fügt eine eindeutige Zahl hinzu, welche die einzelnen Desktops identifiziert. Weitere Informationen finden Sie unter „Verwenden eines Benennungsmusters für automatisierte Desktop-Pools“, auf Seite 122.	Sie geben eine Liste von Desktop-Namen an. In einem Pool mit dedizierter Zuweisung können Sie Benutzer und Desktops einander zuordnen, indem Sie die Benutzernamen mit den Desktop-Namen aufführen. Weitere Informationen finden Sie unter „Angeben einer Liste von Desktop-Namen“, auf Seite 121.
Pool-Größe	Sie geben eine maximale Anzahl an Desktops an.	Ihre Liste mit Desktop-Namen legt die Anzahl an Desktops fest.
Hinzufügen von Desktops zum Pool	Sie können die maximale Pool-Größe erhöhen.	Sie können der Liste weitere Desktop-Namen hinzufügen. Weitere Informationen finden Sie unter „Hinzufügen von Desktops zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde“, auf Seite 250.
Bereitstellung nach Bedarf	Verfügbar. View Manager kann einen Desktop für einen Benutzer erstellen und bereitstellen, sobald der Benutzer sich erstmals anmeldet. View Manager kann bei Erstellung des Pools auch alle Desktops erstellen und bereitstellen.	Nicht verfügbar. Bei Erstellung des Pools erstellt View Manager alle in der Liste angegebenen Desktops und stellt diese bereit.
Anfängliche Anpassung	Verfügbar. Bei der Bereitstellung eines Desktops kann View Manager eine von Ihnen ausgewählte Anpassungsspezifikation ausführen.	Verfügbar. Bei der Bereitstellung eines Desktops kann View Manager eine von Ihnen ausgewählte Anpassungsspezifikation ausführen.
Manuelle Anpassung dedizierter Desktops	Zur Anpassung von Desktops und zur Zurückgabe des Desktop-Zugriffs an die Benutzer müssen Sie den Besitz der einzelnen Desktops entfernen und neu zuweisen. Abhängig davon, ob Sie Desktops bei der ersten Anmeldung zuweisen, müssen Sie diese Schritte möglicherweise zweimal durchführen. Sie können Desktops nicht im Wartungsmodus starten. Nach Erstellung des Pools können Sie die Desktops manuell in den Wartungsmodus versetzen.	Sie können Desktops anpassen und testen, ohne den Besitz neu zuzuweisen. Bei der Erstellung des Pools können Sie alle Desktops im Wartungsmodus starten, um Benutzer am Zugriff zu hindern. Sie können die Desktops anpassen und den Wartungsmodus beenden, um Benutzern den Zugriff wieder zu ermöglichen. Weitere Informationen finden Sie unter „Manuelles Anpassen von Desktops“, auf Seite 125.
Dynamische oder feste Pool-Größe	Dynamisch. Wenn Sie in einem Pool mit dedizierter Zuweisung eine Benutzerzuweisung von einem Desktop entfernen, wird der Desktop wieder dem Pool verfügbarer Desktops hinzugefügt. Wenn Sie in einem Pool mit dynamischer Zuweisung die automatische Löschung bei Abmeldung wählen, kann sich die Pool-Größe je nach Anzahl aktiver Benutzersitzungen vergrößern oder verkleinern.	Fest. Der Pool enthält die Anzahl an Desktops, die Sie in der Liste mit Desktop-Namen bereitgestellt haben. Sie können die Einstellung **[Delete desktop on logoff (Desktop bei Abmeldung löschen)]** nicht festlegen, wenn Sie Desktops manuell benennen.

Tabelle 5-16. Manuelles Benennen von Desktops oder Bereitstellen eines Desktop-Benennungsmusters (Fortsetzung)

Funktion	Bereitstellen eines Desktop-Benennungsmusters	Manuelles Benennen von Desktops
Reserve-Desktops	Sie können eine Anzahl an Reserve-Desktops angeben, die View Manager für neue Benutzer eingeschaltet lässt. View Manager erstellt neue Desktops zur Beibehaltung der angegebenen Anzahl. View Manager beendet die Erstellung von Reserve-Desktops bei Erreichen der maximalen Pool-Größe. View Manager lässt die Reserve-Desktops auch dann eingeschaltet, wenn die Betriebsrichtlinie für den Pool auf **[Power off (Ausschalten)]** oder **[Suspend (Anhalten)]** festgelegt ist oder wenn Sie keine Betriebsrichtlinie einstellen.	Sie können eine Anzahl an Reserve-Desktops angeben, die View Manager für neue Benutzer eingeschaltet lässt. View Manager erstellt keine neuen Reserve-Desktops zur Beibehaltung der angegebenen Anzahl. View Manager lässt die Reserve-Desktops auch dann eingeschaltet, wenn die Betriebsrichtlinie für den Pool auf **[Power off (Ausschalten)]** oder **[Suspend (Anhalten)]** festgelegt ist oder wenn Sie keine Betriebsrichtlinie einstellen.
User assignment (Benutzerzuweisung)	Sie können für Pools mit dedizierter Zuweisung und für Pools mit dynamischer Zuweisung ein Benennungsmuster verwenden.	Sie können für Pools mit dedizierter Zuweisung und für Pools mit dynamischer Zuweisung Desktop-Namen angeben. **Hinweis** In einem Pool mit dynamischer Zuweisung können keine Benutzernamen mit Desktop-Namen verknüpft werden. Die Desktops werden den verknüpften Benutzern nicht dediziert zugewiesen. In einem Pool mit dynamischer Zuweisung bleiben alle derzeit ungenutzten Desktops jedem Benutzer zugänglich, der sich anmeldet.

Angeben einer Liste von Desktop-Namen

Sie können einen automatisierten Desktop-Pool durch die manuelle Angabe einer Liste mit Desktop-Namen bereitstellen. Durch diese Benennungsmethode können Sie die Namenskonventionen Ihres Unternehmens verwenden, um die Desktops in einem Pool zu identifizieren.

Wenn Sie Desktop-Namen explizit angeben, werden den Benutzern bekannte Namen basierend auf der Organisation ihres Unternehmens angezeigt, wenn sie sich an Ihren Desktops anmelden.

Folgen Sie bei der manuellen Benennung von Desktops diesen Richtlinien:

- Geben Sie jeden Desktop-Namen in einer separaten Zeile ein.
- Ein Desktop-Name kann bis zu 15 alphanumerische Zeichen umfassen.
- Sie können jedem Desktop-Eintrag einen Benutzernamen hinzufügen. Mithilfe eines Kommas können Sie den Benutzernamen vom Desktop-Namen trennen.

In diesem Beispiel werden zwei Desktops angegeben. Der zweite Desktop ist mit einem Benutzer verknüpft:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Hinweis In einem Pool mit dynamischer Zuweisung können keine Benutzernamen mit Desktop-Namen verknüpft werden. Die Desktops werden den verknüpften Benutzern nicht dediziert zugewiesen. In einem Pool mit dynamischer Zuweisung bleiben alle derzeit ungenutzten Desktops jedem Benutzer zugänglich, der sich anmeldet.

Voraussetzungen

Stellen Sie sicher, dass alle Desktop-Namen eindeutig sind. Sie können nicht die Namen vorhandener virtueller Maschinen in vCenter Server verwenden.

Vorgehensweise

1 Erstellen Sie eine Textdatei mit der Liste der Desktop-Namen.

   Wenn Sie einen Pool mit nur wenigen Desktops erstellen möchten, können Sie die Desktop-Namen direkt im Assistenten zum Hinzufügen von Pools eingeben. Sie müssen keine separate Textdatei erstellen.

2 Starten Sie in View Administrator den Assistenten zum Hinzufügen von Pools, um mit der Erstellung eines automatisierten Desktop-Pools zu beginnen.

3 Wählen Sie auf der Seite mit den Bereitstellungseinstellungen die Option **[Specify names manually (Namen manuell angeben)]** , und klicken Sie auf **[Enter names (Namen eingeben)]** .

4 Kopieren Sie Ihre Liste mit Desktop-Namen in die Seite **[Enter Desktop Names (Desktop-Namen eingeben)]** , und klicken Sie auf **[Next (Weiter)]** .

   Der Assistent zum Eingeben von Desktop-Namen zeigt die Desktop-Liste an und weist mit einem roten **[X]** auf Validierungsfehler hin.

5 Korrigieren Sie ungültige Desktop-Namen.

   a Platzieren Sie Ihren Cursor auf einem ungültigen Namen, um die entsprechende Fehlermeldung im unteren Seitenbereich anzuzeigen.

   b Klicken Sie auf **[Back (Zurück)]** .

   c Bearbeiten Sie die fehlerhaften Namen, und klicken Sie auf **[Next (Weiter)]** .

6 Klicken Sie auf **[Finish (Fertig stellen)]** .

7 (Optional) Wählen Sie **[Start desktops in maintenance mode (Desktops im Wartungsmodus starten)]** .

   Durch diese Option können Sie die Desktops anpassen, bevor Benutzer sich anmelden und sie verwenden können.

8 Folgen Sie den Anweisungen des Assistenten, um die Erstellung des Desktop-Pools abzuschließen.

View Manager erstellt einen Desktop für jeden Namen in der Liste. Wenn ein Eintrag einen Desktop und einen Benutzernamen umfasst, weist View Manager den Desktop dem jeweiligen Benutzer zu.

Nach der Erstellung des Pools können Sie Desktops hinzufügen, indem Sie eine weitere Listendatei mit zusätzlichen Desktop-Namen und Benutzern importieren.

Verwenden eines Benennungsmusters für automatisierte Desktop-Pools

Sie können die Desktops in einem Pool bereitstellen, indem Sie ein Benennungsmuster und die Gesamtzahl an Desktops bereitstellen, die im Pool enthalten sein sollen. Standardmäßig verwendet View Manager Ihr Muster als Präfix in allen Desktop-Namen und hängt eine eindeutige Zahl zur Identifizierung der einzelnen Desktops an.

Länge des Benennungsmusters in einem Desktop-Namen

Für Desktop-Namen gilt eine Begrenzung auf 15 Zeichen, einschließlich des Benennungsmusters und der automatisch generierten Zahl.

Tabelle 5-17. Maximale Länge des Benennungsmusters in einem Desktop-Namen

Festgelegte Anzahl an Desktops im Pool	Maximale Präfixlänge
1-99	13 Zeichen
100-999	12 Zeichen
1.000 oder mehr	11 Zeichen

Namen mit Token fester Länge besitzen unterschiedliche Längenbeschränkungen. Siehe „Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge“, auf Seite 123.

Verwenden eines Tokens in einem Desktop-Namen

Mithilfe eines Tokens können Sie die automatisch generierte Zahl an einer beliebigen anderen Stelle im Namen platzieren. Geben Sie beim Eingeben des Pool-Namens **n**, eingeschlossen von geschweiften Klammern, ein, um das Token zu bezeichnen.

Beispiel: **amber-{n}-desktop**

Wenn View Manager einen Desktop erstellt, ersetzt View Manager **{n}** durch eine eindeutige Zahl.

Sie können ein Token fester Länge generieren, indem Sie **{n:fixed=*Anzahl der Stellen*}** eingeben.

View Manager ersetzt das Token durch Zahlen mit der angegebenen Anzahl an Stellen.

Wenn Sie beispielsweise **amber-{n:fixed=3}** eingeben, ersetzt View Manager **{n:fixed=3}** durch eine dreistellige Zahl und erstellt folgende Desktop-Namen: **amber-001**, **amber-002**, **amber-003** usw.

Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge

Namen mit Token fester Länge sind auf 15 Zeichen beschränkt, einschließlich Ihres Benennungsmusters und der Anzahl an Stellen im Token.

Tabelle 5-18. Maximale Länge des Benennungsmusters bei Verwendung eines Tokens fester Länge

Token fester Länge	Maximale Länge des Benennungsmusters
{n:fixed=1}	14 Zeichen
{n:fixed=2}	13 Zeichen
{n:fixed=3}	12 Zeichen

Beispiel für die Desktop-Benennung

Dieses Beispiel zeigt die Erstellung zweier automatisierter Desktop-Pools, die dieselben Desktop-Namen, jedoch unterschiedliche Zahlensätze verwenden. Die in diesem Beispiel verwendeten Strategien führen zum Erreichen eines bestimmten Benutzerziels und demonstrieren die Flexibilität der Methoden zur Desktop-Benennung.

Das Ziel besteht darin, zwei Pools mit derselben Namenskonvention wie VDIABC-*XX* zu erstellen, wobei *XX* für eine Zahl steht. Jeder Pool enthält einen anderen Satz aufeinander folgender Zahlen. Beispielsweise enthält der erste Pool die Desktops VDIABC-01 bis VDIABC-10. Der zweite Pool enthält die Desktops VDIABC-11 bis VDIABC-20.

Sie können beide Desktop-Benennungsmethoden einsetzen, um dieses Ziel zu erreichen.

- Um einmal feststehende Sätze von Desktops zu erstellen, geben Sie die Desktop-Namen manuell an.
- Um Desktops dynamisch bei der ersten Benutzeranmeldung zu erstellen, stellen Sie ein Benennungsmuster bereit, und verwenden Sie ein Token zum Festlegen der aufeinander folgenden Zahlen.

Manuelles Angeben der Namen

1 Bereiten Sie für den ersten Pool eine Textdatei vor, die eine Liste der Desktop-Namen von VDIABC-01 bis VDIABC-10 enthält.

2 Erstellen Sie den Pool in View Administrator, und geben Sie die Desktop-Namen manuell an.

3 Klicken Sie auf **[Enter Names (Namen eingeben)]** und kopieren Sie Ihre Liste in das Listenfeld **[Enter Desktop Names (Desktop-Namen eingeben)]** .

4 Wiederholen Sie diese Schritte für den zweiten Pool, und verwenden Sie dabei die Namen VDIABC-11 bis VDIABC-20.

Weitere Anleitungen finden Sie unter „Angeben einer Liste von Desktop-Namen“, auf Seite 121.

Nach der Erstellung der Pools können Sie jedem Pool weitere Desktops hinzufügen. Beispielsweise können Sie dem ersten Pool die Desktops VDIABC-21 bis VDIABC-30, und dem zweiten Pool die Desktops VDIABC-31 bis VDIABC-40 hinzufügen. Siehe „Hinzufügen von Desktops zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde“, auf Seite 250.

Bereitstellen eines Benennungsmusters mit einem Token

1 Erstellen Sie den ersten Pool in View Administrator, und verwenden Sie ein Benennungsmuster zum Bereitstellen der Desktop-Namen.

2 Geben Sie im Textfeld für das Benennungsmuster **`VDIABC-0{n}`** ein.

3 Begrenzen Sie die maximale Pool-Größe auf 9.

4 Wiederholen Sie diese Schritte für den zweiten Pool, geben Sie jedoch im Textfeld für das Benennungsmuster **`VDIABC-1{n}`** ein.

Der erste Pool enthält die Desktops VDIABC-01 bis VDIABC-09. Der zweite Pool enthält die Desktops VDIABC-11 bis VDIABC-19.

Alternativ dazu können Sie die Pools so konfigurieren, dass sie jeweils bis zu 99 Desktops enthalten können, indem Sie ein Token fester Länge mit 2 Stellen verwenden:

- Geben Sie für den ersten Pool **`VDIABC-0{n:fixed=2}`** ein.
- Geben Sie für den zweiten Pool **`VDIABC-1{n:fixed=2}`** ein.

Begrenzen Sie die maximale Größe beider Pools auf 99. Durch diese Konfiguration werden Desktops nach einem Benennungsmuster erstellt, bei dem die Desktop-Namen auf eine sequenzielle, dreistellige Zahl enden.

Erster Pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Zweiter Pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

Weitere Informationen zu Benennungsmustern und Token finden Sie unter „Verwenden eines Benennungsmusters für automatisierte Desktop-Pools“, auf Seite 122.

Manuelles Anpassen von Desktops

Nach der Erstellung eines automatisierten Pools können Sie bestimmte Desktops anpassen, ohne den Besitz neu zuzuweisen. Durch das Starten der Desktops im Wartungsmodus können Sie die Desktops ändern und testen, bevor Sie sie den zugewiesenen Benutzern freigeben oder allen berechtigten Benutzern im Pool zur Verfügung stellen.

- Anpassen von Desktops im Wartungsmodus auf Seite 125

  Der Wartungsmodus hindert Benutzer am Zugriff auf ihre Desktops. Wenn Sie Desktops im Wartungsmodus starten, versetzt View Manager jeden Desktop bei seiner Erstellung in den Wartungsmodus.

- Anpassen einzelner Desktops auf Seite 125

  Sie können nach der Erstellung eines Pools einzelne Desktops anpassen, indem Sie die Desktops im Wartungsmodus starten.

Anpassen von Desktops im Wartungsmodus

Der Wartungsmodus hindert Benutzer am Zugriff auf ihre Desktops. Wenn Sie Desktops im Wartungsmodus starten, versetzt View Manager jeden Desktop bei seiner Erstellung in den Wartungsmodus.

In einem Pool mit dedizierter Zuweisung können Sie den Wartungsmodus zum Anmelden an einem Desktop verwenden, ohne den Besitz erneut Ihrem eigenen Administratorkonto zuzuweisen. Nach der Anpassung müssen Sie den Besitz nicht wieder an den Benutzer zurückgeben, der dem Desktop zugewiesen ist.

In einem Pool mit dynamischer Zuweisung können Sie Desktops im Wartungsmodus testen, bevor Benutzern die Anmeldung erlaubt wird.

Um dieselbe Anpassung auf allen Desktops in einem automatisierten Pool durchzuführen, passen Sie die virtuelle Maschine an, die Sie als Vorlage oder übergeordnetes Element vorbereiten. View Manager stellt Ihre Anpassung für alle Desktops bereit. Bei der Erstellung des Pools können Sie auch eine Sysprep-Anpassungsspezifikation zum Konfigurieren aller Desktops mit Lizenzierung, Domänenanbindung, DHCP-Einstellungen und anderen Computereigenschaften verwenden.

Hinweis Desktops können im Wartungsmodus gestartet werden, sofern Sie die Desktop-Namen für den Pool manuell angeben. Wenn Sie zur Benennung der Desktops ein Benennungsmuster verwenden, ist dies nicht möglich.

Anpassen einzelner Desktops

Sie können nach der Erstellung eines Pools einzelne Desktops anpassen, indem Sie die Desktops im Wartungsmodus starten.

Vorgehensweise

1. Erstellen Sie zunächst in View Administrator einen automatisierten Desktop-Pool, indem Sie den Assistenten zum Hinzufügen von Pools starten.
2. Wählen Sie auf der Seite mit den Bereitstellungseinstellungen die Option **[Specify names manually (Namen manuell angeben)]** .
3. Wählen Sie **[Start desktops in maintenance mode (Desktops im Wartungsmodus starten)]** .
4. Schließen Sie den Assistenten zum Hinzufügen von Pools ab, um den Desktop-Pool zu erstellen.
5. Melden Sie sich in vCenter Server bei den einzelnen virtuellen Desktop-Maschinen an, passen Sie sie an, und testen Sie sie.

   Sie können die Desktops manuell oder über eine Windows-Standardsoftware zur Systemverwaltung anpassen, beispielsweise Altiris, SMS, LanDesk oder BMC.

6 Wählen Sie in View Administrator den Desktop-Pool aus.

7 Klicken Sie auf **[Select all (Alle auswählen)]** , oder wählen Sie mithilfe des Filtertools bestimmte Desktops aus, die Sie für Ihre Benutzer freigeben möchten.

8 Klicken Sie auf **[More Commands (Weitere Befehle)] > [Exit Maintenance Mode (Wartungsmodus beenden)]** .

Weiter

Benachrichtigen Sie Ihre Benutzer darüber, dass sie sich an ihren Desktops anmelden können.

Desktop- und Pool-Einstellungen

Bei der Konfiguration von automatisierten Pools mit vollständigen virtuellen Maschinen, Linked-Clone-Desktop-Pools, manuellen Desktop-Pools und Microsoft-Terminaldienste-Pools müssen Sie Desktop- und Pool-Einstellungen angeben. Nicht alle Einstellungen gelten für alle Typen von Desktop-Pools.

Tabelle 5-19. Beschreibungen der Desktop- und Pool-Einstellungen

Einstellung	Optionen
State (Status)	■ **[Enabled (Aktiviert)]** . Nach seiner Erstellung wird der Desktop-Pool aktiviert und kann sofort verwendet werden. ■ **[Disabled (Deaktiviert)]** . Nach seiner Erstellung ist der Desktop-Pool deaktiviert und nicht verfügbar und die Bereitstellung für den Pool ist unterbrochen. Diese Einstellung ist geeignet, wenn Sie nach der Bereitstellung noch verschiedene Aufgaben ausführen möchten, z.B. ein Testing oder eine grundlegende Wartung.
Connection Server Restrictions (Einschränkungen für Connection Server)	■ **[None (Keine)]** . Der Desktop-Pool ist für jede View Connection Server-Instanz zugänglich. ■ **[With tags (Mit Kennzeichen)]** . Wählen Sie mindestens ein View Connection Server-Kennzeichen aus, um den Zugriff auf den Desktop-Pool nur für View Connection Server-Instanzen zuzulassen, die über diese Kennzeichen verfügen. Sie können die Kontrollkästchen verwenden, um mehrere Kennzeichen auszuwählen.
Betriebsrichtlinie für Remote-Desktops	Legt fest, wie eine virtuelle Maschine sich beim Abmelden eines Benutzers vom verknüpften Desktop verhält. Beschreibungen der Betriebsrichtlinienoptionen finden Sie unter „Betriebsrichtlinien für Desktop-Pools“, auf Seite 132. Weitere Informationen über die Auswirkungen von Betriebsrichtlinien auf automatisierte Pools finden Sie unter „Einstellen von Betriebsrichtlinien für Desktop-Pools“, auf Seite 132.
Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)	■ **[Immediately (Sofort)]** . Benutzer werden sofort nach der Verbindungstrennung abgemeldet. ■ **[Never (Nie)]** . Benutzer werden nie abgemeldet. ■ **[After (Nach)]** . Zeitspanne, nach der Benutzer abgemeldet werden, wenn sie die Verbindung trennen. Geben Sie die Dauer in Minuten ein. Die Abmeldezeit gilt für zukünftige Verbindungstrennungen. Wenn eine Desktop-Sitzung bereits getrennt war, als Sie die Abmeldezeit festlegten, startet die Abmeldedauer für diesen Benutzer, wenn Sie die Abmeldezeit festlegen, und nicht zu dem Zeitpunkt, als die Trennung ursprünglich stattfand. Wenn Sie hierfür beispielsweise fünf Minuten festlegen und eine Sitzung vor 10 Minuten getrennt wurde, meldet View diese Sitzung fünf Minuten nach dem Festlegen des Werts ab.

Tabelle 5-19. Beschreibungen der Desktop- und Pool-Einstellungen (Fortsetzung)

Einstellung	Optionen
Allow users to reset their desktops (Benutzern das Zurücksetzen ihrer Desktops gestatten)	Ermöglicht Benutzern das Zurücksetzen ihrer eigenen Desktops ohne Unterstützung des Administrators.
Allow multiple sessions per user (Mehrere Sitzungen pro Benutzer zulassen)	Ermöglicht Benutzern das Herstellen gleichzeitiger Verbindungen mit mehreren Desktops im Pool.
Delete desktop after logoff (Desktop nach Abmeldung löschen)	Geben Sie an, ob auf vollständigen virtuellen Maschinen basierte Desktops mit dynamischer Zuweisung gelöscht werden sollen. ■ **[No (Nein)]** . Virtuelle Maschinen verbleiben nach der Abmeldung des Benutzers im Desktop-Pool. ■ **[Yes (Ja)]** . Virtuelle Maschinen werden ausgeschaltet und gelöscht, sobald Benutzer sich abmelden.
Delete or refresh desktop on logoff (Desktop bei Abmeldung löschen oder aktualisieren)	Wählen Sie aus, ob Linked-Clone-Desktops mit dynamischer Zuordnung gelöscht, aktualisiert oder unverändert belassen werden sollen. ■ **[Never (Nie)]** . Virtuelle Maschinen verbleiben nach der Abmeldung des Benutzers im Desktop-Pool und werden nicht aktualisiert. ■ **[Delete Immediately (Sofort löschen)]** . Virtuelle Maschinen werden ausgeschaltet und gelöscht, sobald Benutzer sich abmelden. Wenn sich Benutzer abmelden, versetzt View Manager virtuelle Maschinen sofort in den Zustand `Deleting (Löschen)`. ■ **[Refresh Immediately (Sofort aktualisieren)]** . Virtuelle Maschinen werden bei Benutzerabmeldung sofort aktualisiert. Wenn sich Benutzer abmelden, versetzt View Manager virtuelle Maschinen sofort in den Wartungsmodus, damit andere Benutzer sich zu Beginn des Aktualisierungsvorgangs nicht anmelden können.

Tabelle 5-19. Beschreibungen der Desktop- und Pool-Einstellungen (Fortsetzung)

Einstellung	Optionen
Refresh OS disk after logoff (Betriebssystemfestplatte nach Abmelden aktualisieren)	Wählen Sie aus, ob und wann die Betriebssystemfestplatten für Linked-Clone-Desktops mit dedizierter Zuweisung aktualisiert werden sollen. ■ **[Never (Nie)]** . Die Betriebssystemfestplatte wird nie aktualisiert. ■ **[Always (Immer)]** . Die Betriebssystemfestplatte wird bei jeder Abmeldung des Benutzers aktualisiert. ■ **[Every (Alle)]** . Die Betriebssystemfestplatte wird in regelmäßigen Intervallen aus einer bestimmten Anzahl an Tagen aktualisiert. Geben Sie die Anzahl der Tage ein. Die Anzahl der Tage wird von der letzten Aktualisierung oder von der erstmaligen Bereitstellung an berechnet, sofern noch keine Aktualisierung vorgenommen wurde. Wird der Wert z. B. mit **3** Tagen angegeben und es sind drei Tage seit der letzten Aktualisierung vergangen, wird der Desktop aktualisiert, nachdem sich der Benutzer abgemeldet hat. ■ **[At (Bei)]** . Die Betriebssystemfestplatte wird aktualisiert, wenn die aktuelle Größe einen bestimmten Prozentsatz der maximal zulässigen Größe erreicht. Die maximale Größe der Betriebssystemfestplatte eines vernküpften Klons entspricht der Größe der Betriebssystemfestplatte des Replikats. Geben Sie den Prozentsatz ein, bei dem der Aktualisierungsvorgang stattfinden soll. Mit der Option **[At (Bei)]** wird die Größe der Linked-Clone-Betriebssystemfestplatte im Datenspeicher mit der maximal zulässigen Größe verglichen. Der Prozentsatz der Festplattennutzung stellt nicht die Festplattennutzung dar, die möglicherweise im Desktop-Gastbetriebssystem angezeigt wird. Wenn Sie die Betriebssystemfestplatten in einem Linked-Clone-Pool mit dedizierter Zuweisung aktualisieren, bleiben die persistenten View Composer-Festplatten unberührt.
Default display protocol (Standardanzeigeprotokoll)	Wählen Sie das Anzeigeprotokoll, das View Connection Server zur Kommunikation mit View Client verwenden soll. **PCoIP** – Die Standardoption, sofern sie unterstützt wird. PCoIP wird als Anzeigeprotokoll für VM-Desktops und physische Maschinen mit Teradici-Hardware unterstützt. PCoIP ermöglicht ein optimales PC-Erlebnis bei der Bereitstellung von Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN. **Microsoft RDP** – Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht.
Allow users to choose a protocol (Benutzern die Wahl des Protokolls erlauben)	Erlauben Sie Benutzern das Außerkraftsetzen des Standardanzeigeprotokolls für ihre Desktops über View Client.

Tabelle 5-19. Beschreibungen der Desktop- und Pool-Einstellungen (Fortsetzung)

Einstellung	Optionen
Windows 7-3D-Rendering	Sie können auswählen, ob das 3D-Grafikrendern aktiviert werden soll, wenn Ihr Pool Windows 7-Desktops enthält, auf denen vSphere 5.0 oder neuer ausgeführt wird, PCoIP das ausgewählte Protokoll ist und für die EinstellungAllow users to choose protocol (Benutzern die Wahl des Protokolls erlauben) die Option **[No (Nein)]** festgelegt ist. Mit Windows 7-3D-Rendering können die Benutzer die Vorteile von Grafikverbesserungen nutzen, die durch Anwendungen wie AERO, Microsoft Office 2010 und Google Earth bereitgestellt werden. Wenn Ihre View-Bereitstellung nicht mit vSphere 5.0 oder höher ausgeführt wird, ist diese Einstellung nicht verfügbar und in View Administrator nicht aktiv. Wenn Sie diese Funktion auswählen, können Sie die Größe des VRAM konfigurieren, der den Desktops im Pool zugeordnet wird. Sie können höchstens zwei Monitore für Ihre View-Desktops auswählen. Die maximale Auflösung eines Monitors beträgt 1920x1200 Pixel. Dieser Wert kann nicht konfiguriert werden. **Hinweis** Sie müssen die vorhandenen virtuellen Maschinen aus- und wieder einschalten, damit diese Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese Einstellung nicht übernommen. Weitere Informationen finden Sie unter „Konfigurieren von 3D-Rendern auf Windows 7-Desktops“, auf Seite 131.
Max number of monitors (Maximale Anzahl an Monitoren)	Wenn Sie PCoIP als Anzeigeprotokoll verwenden, können Sie die maximale Anzahl an Monitoren auswählen, auf denen Benutzer den Desktop anzeigen können. Wenn die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) nicht ausgewählt ist, bezieht sich die Einstellung „Max number of monitors (Maximale Anzahl an Monitoren)“ auf die Größe des VRAM, der den Desktops im Pool zugeordnet ist. Wenn Sie die Monitoranzahl erhöhen, wird in den verknüpften ESX-Hosts mehr Arbeitsspeicher belegt. Wenn die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) ausgewählt ist, können Sie höchstens zwei Monitore auswählen. **Hinweis** Sie müssen die vorhandenen virtuellen Maschinen aus- und wieder einschalten, damit diese Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese Einstellung nicht übernommen.

Tabelle 5-19. Beschreibungen der Desktop- und Pool-Einstellungen (Fortsetzung)

Einstellung	Optionen
Max resolution of any one monitor (Max. Auflösung eines Monitors)	Wenn Sie PCoIP als Anzeigeprotokoll verwenden und dabei die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) nicht auswählen, sollten Sie die maximale Auflösung jedes Monitors angeben. Wenn die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) nicht ausgewählt ist, bezieht sich die Einstellung Max resolution of any one monitor (Max. Auflösung eines Monitors) auf die Größe des VRAM, der den Desktops im Pool zugeordnet ist. Wenn Sie die Auflösung erhöhen, wird in den verknüpften ESX-Hosts mehr Arbeitsspeicher belegt. Wenn die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendering) ausgewählt ist, können Sie die maximale Auflösung eines Monitors nicht ändern. Die Auflösung wird auf 1920x1200 Pixel festgesetzt. **Hinweis** Sie müssen die vorhandenen virtuellen Maschinen aus- und wieder einschalten, damit diese Einstellung übernommen wird. Durch einen Neustart einer virtuellen Maschine wird diese Einstellung nicht übernommen.
Adobe Flash quality (Adobe Flash-Qualität)	Legt die Qualität der Adobe Flash-Inhalte fest, die auf Webseiten angezeigt werden. ■ **[Do not control (Keine Festlegung)]** . Die Qualität wird durch die Webseiteneinstellungen bestimmt. ■ **[Low (Niedrig)]** . Mit dieser Einstellung werden die höchsten Bandbreiteeinsparungen erzielt. Wenn keine Qualitätsstufe angegeben ist, verwendet das System die Standardeinstellung **[Low (Niedrig)]** . ■ **[Medium (Mittel)]** . Mit dieser Einstellung werden mittlere Bandbreiteeinsparungen erzielt. ■ **[High (Hoch)]** . Mit dieser Einstellung werden die geringsten Bandbreiteeinsparungen erzielt. Weitere Informationen finden Sie unter „Adobe Flash-Qualität und -Drosselung“, auf Seite 253.
Adobe Flash throttling (Adobe Flash-Drosselung)	Legt die Frame-Rate von Adobe Flash-Filmen fest. Wenn Sie diese Einstellung aktivieren, können Sie die Anzahl der pro Sekunde angezeigten Frames verringern oder steigern, indem Sie eine aggressive Stufe auswählen. ■ **[Disabled (Deaktiviert)]** . Es erfolgt keine Drosselung. Das Zeitgeberintervall bleibt unverändert. ■ **[Conservative (Konservativ)]** . Das Zeitgeberintervall lautet 100 Millisekunden. Diese Einstellung führt zur geringsten Anzahl an verworfenen Frames. ■ **[Moderate (Mittel)]** . Das Zeitgeberintervall lautet 500 Millisekunden. ■ **[Aggressive (Aggressiv)]** . Das Zeitgeberintervall lautet 2500 Millisekunden. Diese Einstellung führt zur höchsten Anzahl an verworfenen Frames. Weitere Informationen finden Sie unter „Adobe Flash-Qualität und -Drosselung“, auf Seite 253.

Hinweis Eigenschaften für lokale Desktops werden erst nach dem erneuten Einchecken der Desktops wirksam.

Konfigurieren von 3D-Rendern auf Windows 7-Desktops

Wenn Sie einen Windows 7-Desktop-Pool erstellen, können Sie das 3D-Grafikrendering für Ihre Desktops konfigurieren. Wenn Sie diese Desktop-Einstellung auswählen, können die Benutzer die Vorteile von Grafikverbesserungen nutzen, die durch Anwendungen wie AERO, Microsoft Office 2010 und Google Earth bereitgestellt werden.

Um 3D-Grafikrendering zu aktivieren, muss Ihre Poolbereitstellung die folgenden Anforderungen erfüllen:

- Die Desktops müssen unter Hosts mit ESXi 5.0 oder höher ausgeführt und von vCenter Server 5.0-Software oder höher verwaltet werden.
- Die Desktops müssen Windows 7 oder höher sein.
- Auf den Desktops muss virtuelle Hardware V8 oder höher installiert sein.
- Der Pool muss PCoIP als Standardanzeigeprotokoll verwenden.
- Den Benutzern darf keine Berechtigung zur Auswahl ihres eigenen Protokolls gewährt werden

Wenn Sie die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) aktivieren, können Sie die Größe des VRAM konfigurieren, der den Desktops im Pool zugewiesen ist, indem Sie den Schieberegler im Dialogfeld Configure VRAM for 3D guests (VRAM für 3D-Gäste konfigurieren) bewegen. Die Standard-VRAM-Größe beträgt 64 MB, die Mindestgröße. Sie können die Größe des VRAM bis zu einem Maximum von 128 MB konfigurieren.

Die VRAM-Einstellungen, die Sie in View Administrator konfigurieren, haben Vorrang vor den VRAM-Einstellungen, die für virtuelle Maschinen in vSphere Client konfiguriert werden können.

Wenn Sie die Einstellung Windows 7 3D Rendering (Windows 7-3D-Rendern) aktivieren, können Sie die Einstellung Max number of monitors (Maximale Anzahl an Monitoren) auf einen oder zwei Monitore setzen. Sie können nicht mehr als zwei Monitore auswählen. Weiterhin beträgt die maximale Auflösung für jeden Monitor 1920x1200 Pixel. Dieser Wert kann nicht konfiguriert werden.

Verhindern vom Zugriff auf View-Desktops durch RDP

In bestimmten View-Umgebungen ist die Verhinderung eines Zugriffs auf View-Desktops durch das RDP-Anzeigeprotokoll eine Priorität. Sie können die Benutzer und Administratoren beim Zugriff auf View-Desktops von der RDP-Verwendung abhalten, indem Sie die Pool-Einstellungen und die Gruppenrichtlinieneinstellungen konfigurieren.

Hinweis Remote-Desktop-Dienste, in Windows XP-Systemen als „Terminaldienste“ bezeichnet, müssen auf der virtuellen Maschine gestartet werden, die Sie zur Erstellung von Pools und auf View-Desktops verwenden. Die Remote-Desktop-Dienste sind erforderlich für die Installation von View Agent, SSO und andere View-Sitzungsverwaltungsvorgänge.

Voraussetzungen

Stellen Sie sicher, dass die Datei „VMware View Agent Configuration Administrative Template (Administrative Vorlage zur VMware View Agent-Konfiguration)“ in Active Directory installiert ist. Siehe „Verwenden der Gruppenrichtlinien-ADM-Vorlagendateien für View“, auf Seite 169.

Vorgehensweise

1 Wählen Sie PCoIP als das Anzeigeprotokoll, das View Connection Server zur Kommunikation mit View-Clients verwenden soll.

Option	Beschreibung
Erstellung eines Desktop-Pools	a Starten Sie in View Administrator den Assistenten Add Pool (Pool hinzufügen). b Wählen Sie auf der Seite für die Desktopeinstellungen **[PCoIP]** als Standardanzeigeprotokoll aus.
Bearbeiten eines bestehenden Desktop-Pools	a Wählen Sie in View Administrator den Desktop-Pool aus und klicken Sie auf **[Edit (Bearbeiten)]** . b Wählen Sie die Registerkarte Pool Settings (Pool-Einstellungen) und legen Sie **[PCoIP]** als Standardanzeigeprotokoll fest.

2 Wählen Sie für die Einstellung **[Allow users to choose protocol (Benutzern die Wahl des Protokolls erlauben)]** die Option **[No (Nein)]** .

3 Verhindern Sie die direkte Verbindung von Nicht-View-Clients mit View-Desktops über RPD, indem Sie die Gruppenrichtlinieneinstellung `AllowDirectRDP(Direkte RDP-Verbindung zulassen)` deaktivieren.

   a Öffnen Sie auf Ihrem Active Directory-Server die Konsole zur Gruppenrichtlinienverwaltung und wählen Sie **[Computer Configuration (Computerkonfiguration)] > [Administrative Templates (Administrative Vorlagen)] > [VMware View Agent Configuration (VMware View Agent-Konfiguration)]** aus.

   b Deaktivieren Sie die Einstellung `AllowDirectRDP(Direkte RDP-Verbindung zulassen)`.

Einstellen von Betriebsrichtlinien für Desktop-Pools

Sie können eine Betriebsrichtlinie für die virtuellen Maschinen in einem Desktop-Pool konfigurieren, wenn die virtuellen Maschinen über vCenter Server verwaltet werden.

Über Betriebsrichtlinien wird gesteuert, wie eine virtuelle Maschine sich verhält, wenn der damit verknüpfte Desktop nicht verwendet wird. Ein Desktop wird als nicht verwendet betrachtet, bevor ein Benutzer sich anmeldet und nachdem ein Benutzer die Verbindung trennt oder sich abmeldet. Betriebsrichtlinien steuern außerdem, wie sich eine virtuelle Maschine nach Abschluss von Verwaltungsaufgaben wie der Aktualisierung, Neuzusammenstellung und Neuverteilung verhält.

Sie konfigurieren Betriebsrichtlinien, wenn Sie Desktop-Pools in View Administrator erstellen oder bearbeiten. Siehe Kapitel 5, „Erstellen von Desktop-Pools“, auf Seite 83 oder „Verwalten von Desktop-Pools“, auf Seite 247.

Hinweis Für Desktop-Pools mit nicht verwalteten Desktops können Sie keine Betriebsrichtlinien konfigurieren.

Betriebsrichtlinien für Desktop-Pools

Über Betriebsrichtlinien wird gesteuert, wie eine virtuelle Maschine sich verhält, wenn der damit verknüpfte View-Desktop nicht verwendet wird.

Sie legen Betriebsrichtlinien fest, wenn Sie einen Desktop-Pool erstellen oder bearbeiten. Tabelle 5-20 beschreibt die verfügbaren Betriebsrichtlinien.

Tabelle 5-20. Betriebsrichtlinien

Betriebsrichtlinie	Beschreibung
[Take no power action (Keine Betriebsaktion vornehmen)]	View Manager wendet nach der Abmeldung des Benutzers keine Betriebsrichtlinie an. Diese Einstellung hat zwei Konsequenzen. ■ View Manager ändert nach der Abmeldung eines Benutzers den Betriebsstatus der virtuellen Maschine nicht. Wenn ein Benutzer die virtuelle Maschine beispielsweise herunterfährt, bleibt die virtuelle Maschine ausgeschaltet. Wenn ein Benutzer sich abmeldet, ohne die virtuelle Maschine herunterzufahren, bleibt die virtuelle Maschine eingeschaltet. Die virtuelle Maschine wird neu gestartet, wenn ein Benutzer sich mit dem Desktop verbindet. ■ View Manager setzt keinen Betriebsstatus durch, nachdem eine Verwaltungsaufgabe abgeschlossen wurde. Beispielsweise kann ein Benutzer sich abmelden, ohne die virtuelle Maschine herunterzufahren. Die virtuelle Maschine bleibt eingeschaltet. Wenn eine geplante Neuzusammenstellung stattfindet, wird die virtuelle Maschine ausgeschaltet. Nach Abschluss der Neuzusammenstellung unternimmt View Manager keine Schritte zum Ändern des Betriebsstatus der virtuellen Maschine. Sie bleibt ausgeschaltet.
[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]	Die virtuelle Maschine bleibt auch dann eingeschaltet, wenn sie nicht verwendet wird. Wenn ein Benutzer die virtuelle Maschine herunterfährt, wird sie sofort neu gestartet. Die virtuelle Maschine wird außerdem nach Abschluss einer Verwaltungsaufgabe wie z.B. einer Aktualisierung, Neuzusammenstellung oder Neuverteilung neu gestartet. Wählen Sie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** , wenn Sie Batch-Prozesse oder Systemverwaltungs-Tools ausführen, welche zu bestimmten Zeiten auf die virtuellen Maschinen zugreifen müssen.
[Anhalten]	Die virtuelle Maschine wird angehalten, wenn sich ein Benutzer abmeldet, jedoch nicht, wenn ein Benutzer die Verbindung trennt.
[Power Off (Ausschalten)]	Die virtuelle Maschine wird heruntergefahren, wenn sich ein Benutzer abmeldet, jedoch nicht, wenn ein Benutzer die Verbindung trennt.

HINWEIS Wenn Sie einen Desktop einem manuellen Pool hinzufügen, schaltet View Manager den Desktop ein, um sicherzustellen, dass er vollständig konfiguriert ist. Dies geschieht selbst dann, wenn Sie die Betriebsrichtlinie **[Power off (Ausschalten)]** oder **[Take No Power Action on Logoff (Bei Abmeldung keine Betriebsaktion durchführen)]** auswählen. Sobald der View Agent konfiguriert ist, wird er als bereit markiert, und es gelten die normalen Betriebsverwaltungseinstellungen für den Pool.

Für manuelle Pools mit Desktops, die über vCenter Server verwaltet werden, schaltet View Manager einen Reserve-Desktop ein, damit die Benutzer sich verbinden können. Der Reserve-Desktop wird unabhängig davon eingeschaltet, welche Betriebsrichtlinie in Kraft ist.

Tabelle 5-21 beschreibt, wann View Manager die konfigurierte Betriebsrichtlinie anwendet.

Tabelle 5-21. Zeitpunkt der Anwendung der Betriebsrichtlinie durch View Manager

Typ des Desktop-Pools	Anwendung der Betriebsrichtlinie
Manueller Pool mit einem Desktop (über vCenter Server verwaltete virtuelle Maschine)	Betriebsvorgänge werden durch die Sitzungsverwaltung initiiert. Die virtuelle Maschine wird eingeschaltet, wenn ein Benutzer den Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet. **Hinweis** Die Richtlinie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** wird immer angewendet, unabhängig davon, ob der Pool mit einem einzigen Desktop eine dynamische oder dedizierte Zuweisung verwendet und ob der Desktop zugewiesen oder nicht zugewiesen ist.
Automatisierter Pool mit dedizierter Zuweisung	Wird nur auf nicht zugewiesene Desktops angewendet. Auf zugewiesenen Desktops werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Virtuelle Maschinen werden eingeschaltet, wenn ein Benutzer einen zugewiesenen Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet. **Hinweis** Die Richtlinie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** gilt für zugewiesene und nicht zugewiesene Desktops.
Automatisierter Pool mit dynamischer Zuweisung	Wird angewendet, wenn ein Desktop nicht verwendet wird und nachdem ein Benutzer sich abgemeldet hat. Wenn Sie die Betriebsrichtlinie **[Power off (Ausschalten)]** oder **[Suspend (Anhalten)]** für einen Desktop-Pool mit dynamischer Zuweisung konfigurieren, stellen Sie **[Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)]** auf **[Immediately (Sofort)]** , um verworfene oder verwaiste Sitzungen zu verhindern.
Manueller Pool mit dedizierter Zuweisung	Wird nur auf nicht zugewiesene Desktops angewendet. Auf zugewiesenen Desktops werden Betriebsvorgänge von der Sitzungsverwaltung initiiert. Virtuelle Maschinen werden eingeschaltet, wenn ein Benutzer einen zugewiesenen Desktop anfordert, und ausgeschaltet oder angehalten, wenn der Benutzer sich abmeldet. **Hinweis** Die Richtlinie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** gilt für zugewiesene und nicht zugewiesene Desktops.
Manueller Pool mit dynamischer Zuweisung	Wird angewendet, wenn ein Desktop nicht verwendet wird und nachdem ein Benutzer sich abgemeldet hat. Wenn Sie die Betriebsrichtlinie **[Power off (Ausschalten)]** oder **[Suspend (Anhalten)]** für einen Desktop-Pool mit dynamischer Zuweisung konfigurieren, stellen Sie **[Automatic logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)]** auf **[Immediately (Sofort)]** , um verworfene oder verwaiste Sitzungen zu verhindern.

Wie View Manager die konfigurierte Betriebsrichtlinie auf automatisierte Pools anwendet, hängt davon ab, ob ein Desktop verfügbar ist. Weitere Informationen finden Sie unter „Auswirkungen von Betriebsrichtlinien auf automatisierte Pools“, auf Seite 135.

Auswirkungen von Betriebsrichtlinien auf automatisierte Pools

Wie View die konfigurierte Betriebsrichtlinie auf automatisierte Pools anwendet, hängt davon ab, ob ein View-Desktop verfügbar ist.

Ein Desktop in einem automatisierten Pool wird als verfügbar betrachtet, wenn er den folgenden Kriterien entspricht:

- Desktop ist aktiv
- Desktop enthält keine Benutzersitzung
- Desktop ist keinem Benutzer zugewiesen

Der auf dem Desktop ausgeführte View Agent-Dienst bestätigt View Connection Server die Verfügbarkeit des Desktops.

Bei der Konfiguration eines automatisierten Pools können Sie die Mindest- und die Höchstzahl an bereitzustellenden virtuellen Maschinen sowie die Anzahl an Reserve-Desktops angeben, die zu jedem Zeitpunkt eingeschaltet bleiben und zur Verfügung stehen müssen.

Beispiele für Betriebsrichtlinien für automatisierte Pools mit dynamischer Zuweisung

Wenn Sie einen automatisierten Pool mit dynamischer Zuweisung konfigurieren, können Sie festlegen, dass eine bestimmte Anzahl an View-Desktops zu jedem Zeitpunkt zur Verfügung stehen muss. Die verfügbaren Reserve-Desktops sind unabhängig von der Betriebsrichtlinieneinstellung jederzeit eingeschaltet.

Betriebsrichtlinie – Beispiel 1

Tabelle 5-22 beschreibt den automatisierten Pool mit dynamischer Zuweisung in diesem Beispiel. Der Pool verwendet ein Desktop-Benennungsmuster, um die Desktops bereitzustellen und zu benennen.

Tabelle 5-22. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 1

Desktop-Pool-Einstellung	Wert
Number of desktops (minimum) (Anzahl an Desktops (Mindestzahl))	10
Number of desktops (maximum) (Anzahl an Desktops (Höchstzahl))	20
Number of spare, powered-on desktops (Anzahl an eingeschalteten Reserve-Desktops)	2
Betriebsrichtlinie für Remote-Desktops	Anhalten

Bei Bereitstellung dieses Desktop-Pools werden zehn Desktops erstellt, zwei Desktops werden eingeschaltet und stehen sofort zur Verfügung, und acht Desktops befinden sich im angehaltenen Zustand.

Für jeden neuen Benutzer, der sich mit dem Pool verbindet, wird ein Desktop eingeschaltet, um die Anzahl an verfügbaren Reserve-Desktops zu erhalten. Wenn mehr als acht Benutzer verbunden sind, werden weitere Desktops bis zur Höchstzahl von 20 erstellt, um die Anzahl an Reserve-Desktops beizubehalten. Nach Erreichen der Höchstzahl bleiben die Desktops der ersten zwei Benutzer, die ihre Verbindung trennen, eingeschaltet, um die Anzahl an Reserve-Desktops zu erhalten. Die Desktops aller nachfolgenden Benutzer werden der Betriebsrichtlinie entsprechend angehalten.

Betriebsrichtlinie – Beispiel 2

Tabelle 5-23 beschreibt den automatisierten Pool mit dynamischer Zuweisung in diesem Beispiel. Der Pool verwendet ein Desktop-Benennungsmuster, um die Desktops bereitzustellen und zu benennen.

Tabelle 5-23. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dynamischer Zuweisung – Beispiel 2

Desktop-Pool-Einstellung	Wert
Number of desktops (minimum) (Anzahl an Desktops (Mindestzahl))	5
Number of desktops (maximum) (Anzahl an Desktops (Höchstzahl))	5
Number of spare, powered-on desktops (Anzahl an eingeschalteten Reserve-Desktops)	2
Betriebsrichtlinie für Remote-Desktops	Anhalten

Bei Bereitstellung dieses Desktop-Pools werden fünf Desktops erstellt, zwei Desktops werden eingeschaltet und stehen sofort zur Verfügung, und drei Desktops befinden sich im angehaltenen Zustand.

Wird ein vierter Desktop in diesem Pool angehalten, wird einer der vorhandenen Desktops fortgesetzt. Es wird kein weiterer Desktop eingeschaltet, weil die Höchstzahl an Desktops bereits erreicht ist.

Beispiel für Betriebsrichtlinien für automatisierte Pools mit dedizierter Zuweisung

Im Gegensatz zu einem eingeschalteten View-Desktop in einem automatisierten Pool mit dynamischer Zuweisung steht ein eingeschalteter Desktop in einem automatisierten Pool mit dedizierter Zuweisung nicht unbedingt zur Verfügung. Er ist nur dann verfügbar, wenn der Desktop keinem Benutzer zugewiesen ist.

Tabelle 5-24 beschreibt den automatisierten Pool mit dedizierter Zuweisung in diesem Beispiel.

Tabelle 5-24. Desktop-Pool-Einstellungen für einen automatisierten Pool mit dedizierter Zuweisung – Beispiel

Desktop-Pool-Einstellung	Wert
Number of desktops (minimum) (Anzahl an Desktops (Mindestzahl))	3
Number of desktops (maximum) (Anzahl an Desktops (Höchstzahl))	5
Number of spare, powered-on desktops (Anzahl an eingeschalteten Reserve-Desktops)	2
Betriebsrichtlinie für Remote-Desktops	Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)

Wird dieser Desktop bereitgestellt, werden drei Desktops erstellt und eingeschaltet. Wenn die Desktops in vCenter Server ausgeschaltet werden, werden sie gemäß der Betriebsrichtlinie sofort wieder eingeschaltet.

Nachdem ein Benutzer sich mit einem Desktop im Pool verbunden hat, wird der Desktop dem entsprechenden Benutzer dauerhaft zugewiesen. Nachdem der Benutzer die Verbindung mit dem Desktop getrennt hat, steht der Desktop keinem anderen Benutzer mehr zur Verfügung. Die Richtlinie **[Ensure desktops are always powered on (Desktops müssen immer eingeschaltet sein)]** gilt jedoch weiterhin. Wird der zugewiesene Desktop in vCenter Server ausgeschaltet, wird er sofort wieder eingeschaltet.

Wenn ein anderer Benutzer eine Verbindung herstellt, wird ein zweiter Desktop zugewiesen. Da die Anzahl an Reserve-Desktops unter die Mindestgrenze fällt, sobald sich der zweite Benutzer verbindet, wird ein weiterer Desktop erstellt und eingeschaltet. Bei jeder Zuweisung eines neuen Benutzers wird ein weiterer Desktop erstellt und eingeschaltet, bis die Höchstzahl an Desktops erreicht ist.

Verhindern von Betriebsrichtlinienkonflikten

Wenn Sie eine Betriebsrichtlinie mithilfe von View Administrator konfigurieren, müssen Sie diese mit den Energieoptionen in der Systemsteuerung auf dem Gastbetriebssystem vergleichen, um Betriebsrichtlinienkonflikte zu vermeiden.

Ein View-Desktop ist möglicherweise vorübergehend nicht verfügbar, wenn die für den Desktop der virtuellen Maschine konfigurierte Betriebsrichtlinie nicht mit einer der Energieoptionen kompatibel ist, die für das Gastbetriebssystem konfiguriert wurden. Wenn sich weitere Desktops in demselben Pool befinden, können auch diese betroffen sein.

Die folgende Konfiguration ist ein Beispiel für einen Betriebsrichtlinienkonflikt:

- In View Administrator ist die Betriebsrichtlinie **[Suspend (Anhalten)]** für den Desktop der virtuellen Maschine konfiguriert. Durch diese Richtlinie wird die virtuelle Maschine angehalten, wenn sie nicht verwendet wird.
- In den Energieoptionen in der Systemsteuerung des Gastbetriebssystems ist die Option **[Put the Computer to sleep (Energiesparmodus nach)]** auf drei Minuten festgelegt.

Bei dieser Konfiguration können sowohl View Connection Server als auch das Gastbetriebssystem die virtuelle Maschine anhalten. Durch die Energieoption des Gastbetriebssystems ist die virtuelle Maschine möglicherweise nicht verfügbar, während View Connection Server erwartet, dass sie eingeschaltet ist.

Berechtigen von Benutzern und Gruppen

6

Berechtigungen für Desktop-Pools werden konfiguriert, um zu steuern, auf welche View-Desktops die Benutzer zugreifen dürfen. Mithilfe der Funktion für eingeschränkte Berechtigungen kann der Desktop-Zugriff zudem basierend auf der View Connection Server-Instanz gesteuert werden, mit der sich die Benutzer bei der Auswahl von Desktops verbinden.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen von Berechtigungen zu Desktop-Pools“, auf Seite 139
- „Entfernen von Berechtigungen für einen Desktop-Pool“, auf Seite 140
- „Überprüfen von Berechtigungen für Desktop-Pools“, auf Seite 140
- „Einschränken des Zugriffs auf View-Desktops“, auf Seite 140

Hinzufügen von Berechtigungen zu Desktop-Pools

Bevor Benutzer auf einen View-Desktop zugreifen können, muss ihnen die Berechtigung für die Verwendung eines Desktop-Pools zugewiesen werden.

Voraussetzungen

Erstellen Sie einen Desktop-Pool. Siehe Kapitel 5, „Erstellen von Desktop-Pools“, auf Seite 83.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Wählen Sie den Desktop-Pool aus und klicken Sie auf **[Entitlements (Berechtigungen)]** .

3 Klicken Sie auf **[Add (Hinzufügen)]** , wählen Sie mindestens ein Suchkriterium und klicken Sie auf **[Find (Suchen)]** , um basierend auf den angegebenen Suchkriterien nach Benutzern oder Gruppen zu suchen.

Hinweis Lokale Domänengruppen werden aus Suchergebnissen für Domänen im gemischten Modus herausgefiltert. Sie können Benutzer in lokalen Gruppen der Domäne nicht berechtigen, wenn Ihre Domäne im gemischten Modus konfiguriert ist.

---

4 Wählen Sie die Benutzer oder Gruppen aus, die für die Desktops dieses Pools berechtigt sein sollen, und klicken Sie auf **[OK]** .

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Entfernen von Berechtigungen für einen Desktop-Pool

Sie können Berechtigungen für einen Desktop-Pool entfernen, um den Zugriff auf einen Desktop durch bestimmte Benutzer oder Gruppen zu verhindern.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Wählen Sie den Desktop-Pool aus und klicken Sie auf **[Entitlements (Berechtigungen)]** .

3 Wählen Sie den Benutzer oder die Gruppe, deren Berechtigung entfernt werden soll, und klicken Sie auf **[Remove (Entfernen)]** .

4 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Überprüfen von Berechtigungen für Desktop-Pools

Sie können überprüfen, für welche Desktop-Pools ein Benutzer oder eine Gruppe berechtigt ist.

Vorgehensweise

1 Wählen Sie in View Administrator **[Users and Groups (Benutzer und Gruppen)]** und klicken Sie auf den Benutzer- oder Gruppennamen.

2 Wählen Sie die Registerkarte **[Summary (Übersicht)]** .

Im Fenster mit den Pool-Berechtigungen werden die Pools angezeigt, für die der Benutzer oder die Gruppe derzeit berechtigt ist.

Einschränken des Zugriffs auf View-Desktops

Mithilfe der Funktion für eingeschränkte Berechtigungen kann der Zugriff auf View-Desktops basierend auf der View Connection Server-Instanz eingeschränkt werden, mit der sich die Benutzer bei der Auswahl von Desktops verbinden.

Zum Einschränken von Berechtigungen weisen Sie einer View Connection Server-Instanz ein oder mehrere Kennzeichen zu. Wenn Sie anschließend einen Desktop-Pool konfigurieren, wählen Sie die Kennzeichen der View Connection Server-Instanzen aus, die auf den Desktop-Pool zugreifen können sollen.

Wenn Benutzer sich an einer so konfigurierten View Connection Server-Instanz anmelden, können sie nur auf die Desktop-Pools zugreifen, die mindestens ein übereinstimmendes Kennzeichen oder keine Kennzeichen aufweisen.

- Beispiel für eingeschränkte Berechtigungen auf Seite 141

  In diesem Beispiel wird eine View-Bereitstellung mit zwei View Connection Server-Instanzen gezeigt. Die erste Instanz unterstützt interne Benutzer. Die zweite Instanz wird mit einem Sicherheitsserver kombiniert und unterstützt externe Benutzer.

- Kennzeichenabgleich auf Seite 142

  Die Funktion für eingeschränkte Berechtigungen ermittelt anhand des Kennzeichenabgleichs, ob eine View Connection Server-Instanz auf einen bestimmten Desktop-Pool zugreifen kann.

- Überlegungen und Einschränkungen bei eingeschränkten Berechtigungen auf Seite 143

  Vor der Implementierung von eingeschränkten Berechtigungen müssen bestimmte Überlegungen und Einschränkungen berücksichtigt werden.

- Zuweisen von Kennzeichen zu einer View Connection Server-Instanz auf Seite 143

  Wenn Sie einer View Connection Server-Instanz ein Kennzeichen zuweisen, können Benutzer, die sich mit dieser View Connection Server-Instanz verbinden, lediglich auf Desktop-Pools mit übereinstimmenden oder ohne jegliche Kennzeichen zugreifen.

- Zuweisen von Kennzeichen zu einem Desktop-Pool auf Seite 144

  Wenn Sie einem Desktop-Pool ein Kennzeichen zuweisen, können nur Benutzer, die sich mit einer View Connection Server-Instanz mit übereinstimmendem Kennzeichen verbinden, auf Desktops in diesem Pool zugreifen.

Beispiel für eingeschränkte Berechtigungen

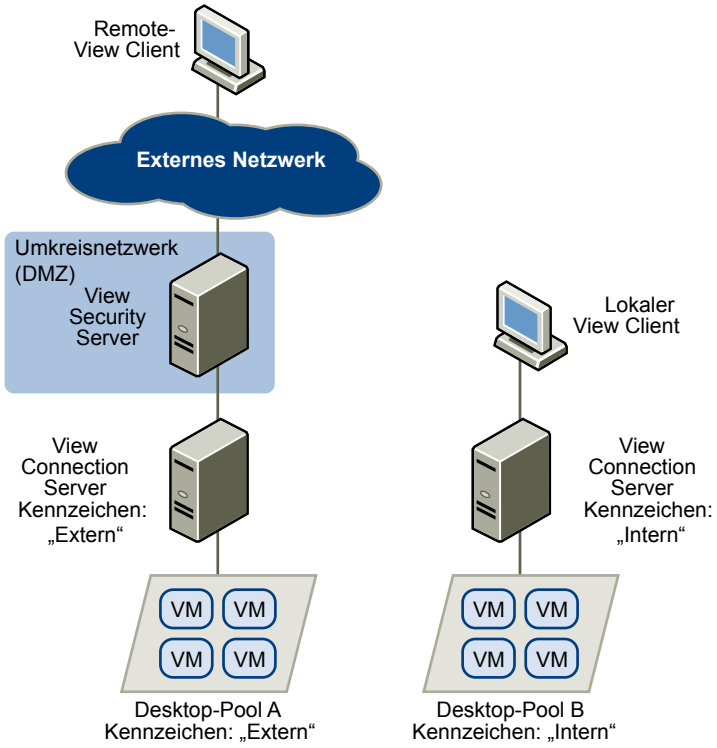
In diesem Beispiel wird eine View-Bereitstellung mit zwei View Connection Server-Instanzen gezeigt. Die erste Instanz unterstützt interne Benutzer. Die zweite Instanz wird mit einem Sicherheitsserver kombiniert und unterstützt externe Benutzer.

Um externe Benutzer am Zugriff auf bestimmte Desktops zu hindern, können Sie eingeschränkte Berechtigungen wie folgt einrichten:

- Weisen Sie das Kennzeichen „Intern“ der View Connection Server-Instanz zu, die die internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der View Connection Server-Instanz zu, die mit dem Sicherheitsserver kombiniert wird und die externen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Intern“ den Desktop-Pools zu, auf die nur interne Benutzer zugreifen dürfen.
- Weisen Sie das Kennzeichen „Extern“ den Desktop-Pools zu, auf die nur externe Benutzer zugreifen dürfen.

Externen Benutzern werden keine als „Intern“ gekennzeichneten Desktop-Pools angezeigt, da sie sich an der als „Extern“ gekennzeichneten View Connection Server-Instanz anmelden. Ebenso können interne Benutzer keine als „Extern“ gekennzeichneten Desktop-Pools sehen, da sie sich an der als „Intern“ gekennzeichneten View Connection Server-Instanz anmelden. Abbildung 6-1 zeigt diese Konfiguration.

Abbildung 6-1. Konfiguration eingeschränkter Berechtigungen



Außerdem können Sie mithilfe eingeschränkter Berechtigungen den Desktop-Zugriff basierend auf der Benutzerauthentifizierungsmethode steuern, die Sie für eine bestimmte View Connection Server-Instanz konfigurieren. Sie können beispielsweise bestimmte Desktop-Pools nur Benutzern zur Verfügung stellen, die sich mit einer Smartcard authentifiziert haben.

Kennzeichenabgleich

Die Funktion für eingeschränkte Berechtigungen ermittelt anhand des Kennzeichenabgleichs, ob eine View Connection Server-Instanz auf einen bestimmten Desktop-Pool zugreifen kann.

Beim Kennzeichenabgleich wird im Wesentlichen ermittelt, ob eine View Connection Server-Instanz mit einem bestimmten Kennzeichen auf einen Desktop-Pool zugreifen kann, der dasselbe Kennzeichen aufweist.

Wenn keine Kennzeichen zugewiesen werden, kann sich dies auch darauf auswirken, ob eine View Connection Server-Instanz auf einen Desktop-Pool zugreifen kann. View Connection Server-Instanzen ohne Kennzeichen können beispielsweise nur auf Desktop-Pools zugreifen, die ebenfalls nicht über Kennzeichen verfügen.

Tabelle 6-1 zeigt, wie die Funktion für eingeschränkte Berechtigungen ermittelt, ob eine View Connection Server-Instanz auf einen Desktop-Pool zugreifen kann.

Tabelle 6-1. Regeln für den Kennzeichenabgleich

View Connection Server	Desktop-Pool	Zugriff zulässig?
Keine Kennzeichen	Keine Kennzeichen	Ja.
Keine Kennzeichen	Mindestens ein Kennzeichen	No (Nein)
Mindestens ein Kennzeichen	Keine Kennzeichen	Ja.
Mindestens ein Kennzeichen	Mindestens ein Kennzeichen	Nur bei übereinstimmenden Kennzeichen

Die Funktion für eingeschränkte Berechtigungen erzwingt nur den Kennzeichenabgleich. Sie müssen Ihre Netzwerktopologie ändern, um für bestimmte Clients die Verbindung über eine bestimmte View Connection Server-Instanz zu erzwingen.

Überlegungen und Einschränkungen bei eingeschränkten Berechtigungen

Vor der Implementierung von eingeschränkten Berechtigungen müssen bestimmte Überlegungen und Einschränkungen berücksichtigt werden.

- Einzelne View Connection Server-Instanzen oder Desktop-Pools können über mehrere Kennzeichen verfügen.
- Mehrere View Connection Server-Instanzen und Desktop-Pools können über dasselbe Kennzeichen verfügen.
- Auf Desktop-Pools ohne Kennzeichen kann von einer beliebigen View Connection Server-Instanz zugegriffen werden.
- View Connection Server-Instanzen ohne Kennzeichen können nur auf Desktop-Pools zugreifen, die ebenfalls nicht über Kennzeichen verfügen.
- Bei Verwendung eines Sicherheitsservers müssen Sie eingeschränkte Berechtigungen für die View Connection Server-Instanz konfigurieren, mit welcher der Sicherheitsserver kombiniert ist. Eingeschränkte Berechtigungen können nicht auf einem Sicherheitsserver konfiguriert werden.
- Sie können das Kennzeichen einer View Connection Server-Instanz nicht ändern oder entfernen, wenn dieses Kennzeichen weiterhin einem Desktop-Pool zugewiesen ist und keine anderen View Connection Server-Instanzen über ein übereinstimmendes Kennzeichen verfügen.
- Eingeschränkte Berechtigungen haben Vorrang vor anderen Desktop-Berechtigungen. Beispiel: Selbst wenn ein Benutzer für den Zugriff auf einen bestimmten Desktop berechtigt ist, kann er nicht auf diesen Desktop zugreifen, wenn das Kennzeichen des Desktop-Pools nicht mit dem Kennzeichen der View Connection Server-Instanz übereinstimmt, mit der sich der Benutzer verbindet.

Zuweisen von Kennzeichen zu einer View Connection Server-Instanz

Wenn Sie einer View Connection Server-Instanz ein Kennzeichen zuweisen, können Benutzer, die sich mit dieser View Connection Server-Instanz verbinden, lediglich auf Desktop-Pools mit übereinstimmenden oder ohne jegliche Kennzeichen zugreifen.

Vorgehensweise

1. Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Servers (Server)]**.
2. Wählen Sie unter **[View Connection Servers (View Connection Server)]** eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]**.
3. Geben Sie im Textfeld **[Tags (Kennzeichen)]** mindestens ein Kennzeichen ein.

   Trennen Sie mehrere Kennzeichen durch ein Komma oder Semikolon.
4. Klicken Sie auf **[OK]**, um Ihre Änderungen zu speichern.

Weiter

Weisen Sie Kennzeichen zu Desktop-Pools zu.

Zuweisen von Kennzeichen zu einem Desktop-Pool

Wenn Sie einem Desktop-Pool ein Kennzeichen zuweisen, können nur Benutzer, die sich mit einer View Connection Server-Instanz mit übereinstimmendem Kennzeichen verbinden, auf Desktops in diesem Pool zugreifen.

Kennzeichen können beim Hinzufügen oder Bearbeiten eines Desktop-Pools zugewiesen werden.

Voraussetzungen

Weisen Sie einer oder mehreren View Connection Server-Instanzen Kennzeichen zu.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie den Pool aus, dem Sie ein Kennzeichen zuweisen möchten.

Option	Aktion
Zuweisen eines Kennzeichens zu einem neuen Pool	Klicken Sie auf **[Add (Hinzufügen)]** , um den Assistenten zum Hinzufügen von Pools zu starten und den Pool anzugeben.
Zuweisen eines Kennzeichens zu einem vorhandenen Pool	Wählen Sie den Pool aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Wechseln Sie zur Seite **[Pool Settings (Pool-Einstellungen)]** .

Option	Aktion
Pool-Einstellungen für einen neuen Pool	Klicken Sie im Assistenten zum Hinzufügen von Pools auf **[Pool Settings (Pool-Einstellungen)]** .
Pool-Einstellungen für einen vorhandenen Pool	Wählen Sie die Registerkarte **[Pool Settings (Pool-Einstellungen)]** .

4 Klicken Sie neben **[Connection Server Restrictions (Connection Server-Einschränkungen)]** auf **[Browse (Durchsuchen)]** und konfigurieren Sie die View Connection Server-Instanzen, die auf den Desktop-Pool zugreifen können.

Option	Aktion
Erteilen von Pool-Zugriff für eine beliebige View Connection Server-Instanz	Wählen Sie **[No Restrictions (Keine Einschränkungen)]** .
Erteilen von Pool-Zugriff nur für entsprechend gekennzeichnete View Connection Server-Instanzen	Wählen Sie **[Restrict to these tags (Auf diese Kennzeichen beschränken)]** und wählen Sie mindestens ein Kennzeichen aus. Sie können die Kontrollkästchen verwenden, um mehrere Kennzeichen auszuwählen.

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Einrichten der Benutzerauthentifizierung 7

View nutzt die vorhandene Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Für zusätzliche Sicherheit können Sie View mit Smartcard- und RSA SecurID-Lösungen integrieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwenden der Smartcard-Authentifizierung“, auf Seite 145
- „Verwenden der Smartcard-Zertifikatssperrüberprüfung“, auf Seite 156
- „Verwenden der RSA SecurID-Authentifizierung“, auf Seite 159
- „Verwenden der Funktion „Anmelden als aktueller Benutzer““, auf Seite 162

Verwenden der Smartcard-Authentifizierung

Sie können eine View Connection Server-Instanz oder einen Sicherheitsserver so konfigurieren, dass sich View-Desktop-Benutzer unter Verwendung von Smartcards authentifizieren können. Smartcards werden manchmal als Common Access Cards (CACs) bezeichnet.

Eine Smartcard ist eine kleine Kunststoffkarte, auf der sich ein Computerchip befindet. Der Chip, der mit einem Mini-Computer vergleichbar ist, bietet eine sichere Datenspeicherung und umfasst u.a. private Schlüssel und Zertifikate für öffentliche Schlüssel.

Bei der Smartcard-Authentifizierung führt ein Benutzer eine Smartcard in einen Smartcard-Leser ein, der mit dem Clientcomputer verbunden ist, und gibt anschließend eine PIN ein. Die Smartcard-Authentifizierung bietet eine zweistufige Authentifizierung, indem einerseits überprüft wird, ob der Benutzer im Besitz der Smartcard ist, und andererseits, ob der Benutzer die erforderliche PIN kennt.

Informationen zu den Hardware- und Softwareanforderungen für die Implementierung der Smartcard-Authentifizierung finden Sie im Dokument *Installation von VMware View*. Ausführliche Informationen zu Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme finden Sie auf der Microsoft TechNet-Website.

Die Smartcard-Authentifizierung wird von View Client für Mac und View Administrator nicht unterstützt. Ausführliche Informationen zur Smartcard-Unterstützung finden Sie im Dokument *Planung der VMware View-Architektur*.

Anmelden über eine Smartcard

Wenn ein Benutzer eine Smartcard in einen Smartcard-Leser einführt, werden die Benutzerzertifikate auf der Smartcard in den lokalen Zertifikatspeicher auf dem Clientsystem kopiert. Die Zertifikate im lokalen Zertifikatspeicher sind für alle auf dem Clientcomputer ausgeführten Anwendungen verfügbar, einschließlich der View Client-Anwendung.

Wenn ein Benutzer eine Verbindung mit einer View Connection Server-Instanz oder einem Sicherheitsserver herstellt, die bzw. der für die Smartcard-Authentifizierung konfiguriert ist, sendet die View Connection Server-Instanz oder der Sicherheitsserver eine Liste vertrauenswürdiger Zertifizierungsstellen an View Client. View Client gleicht die Liste vertrauenswürdiger Zertifizierungsstellen mit den verfügbaren Benutzerzertifikaten ab, wählt ein geeignetes Zertifikat aus und fordert den Benutzer zur Eingabe einer Smartcard-PIN auf. Wenn mehrere gültige Benutzerzertifikate vorhanden sind, fordert View Client den Benutzer zur Auswahl eines Zertifikats auf.

View Client sendet das Benutzerzertifikat an die View Connection Server-Instanz oder den Sicherheitsserver, die bzw. der das Zertifikat basierend auf der Zertifikatvertrauensstellung und der Gültigkeitsdauer überprüft. Benutzer können sich normalerweise erfolgreich authentifizieren, wenn ihr Benutzerzertifikat signiert und gültig ist. Wenn eine Zertifkatssperrüberprüfung konfiguriert ist, können sich Benutzer mit gesperrten Benutzerzertifikaten nicht authentifizieren.

Der Wechsel des Anzeigeprotokolls wird mit der Smartcard-Authentifizierung nicht unterstützt. Zur Änderung des Anzeigeprotokolls nach der Authentifizierung per Smartcard muss sich der Benutzer abmelden und wieder anmelden.

Anmelden an lokalen Desktops über die Offline-Smartcard-Authentifizierung

Über die Offline-Smartcard-Authentifizierung können sich Benutzer an einem lokalen Desktop über eine Smartcard anmelden, wenn der Desktop nicht mit einer View Connection Server-Instanz verbunden ist.

Benutzer müssen sich für die Verwendung der Offline-Smartcard-Authentifizierung über dieselbe Authentifizierungsmethode anmelden, die sie zur Authentifizierung an einer View Connection Server-Instanz bei der letzten Anmeldung verwendet haben. Wenn sich ein Benutzer zum Beispiel mit Smartcard A, ein weiteres Mal mit der Kennwortauthentifizierung und zuletzt mit der Smartcard B angemeldet hat, muss der Benutzer die Smartcard B für die Offline-Smartcard-Authentifizierung verwenden.

Der zuletzt für die Richtlinie zum Entfernen von Smartcards festgelegte Wert wird während der Offline-Smartcard-Authentifizierung erzwungen. Die Richtlinie zum Entfernen von Smartcards legt fest, ob sich Benutzer für den Zugriff auf ihre Desktops nach dem Entfernen ihrer Smartcards erneut authentifizieren müssen. Wenn die Richtlinie zur Trennung von Benutzersitzungen bei Entfernen der Smartcard festgelegt ist, wird das Gastbetriebssystem im View-Desktop bei Entfernen einer Smartcard durch die Benutzer gesperrt. Das View Client-Fenster bleibt geöffnet und Benutzer können **[Options (Optionen)] > [Send Ctrl-Alt-Delete (Strg-Alt-Entf senden)]** auswählen, um sich erneut anzumelden. Die Richtlinie zum Entfernen von Smartcards ist eine View Connection Server-Einstellung.

Konfigurieren der Smartcard-Authentifizierung

Um die Smartcard-Authentifizierung zu konfigurieren, müssen Sie ein Stammzertifikat anfordern und es zu einer Server-Vertrauensspeicherdatei hinzufügen, die View Connection Server-Konfigurationseigenschaften ändern und die Smartcard-Authentifizierungseinstellungen festlegen. Abhängig von Ihrer Umgebung müssen möglicherweise weitere Schritte ausgeführt werden.

Vorgehensweise

1 Anfordern des Stammzertifikats von der Zertifizierungsstelle auf Seite 147

Sie müssen das Stammzertifikat von der Zertifizierungsstelle anfordern, welche die Zertifikate auf den von Ihren Benutzern verwendeten Smartcards signiert hat.

2 Exportieren eines Stammzertifikats aus einem Benutzerzertifikat auf Seite 148

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Benutzerzertifikat oder eine Smartcard mit Zertifikat verfügen, können Sie das Stammzertifikat exportieren, wenn es von ihrem System als vertrauenswürdig eingestuft wird.

3 Hinzufügen des Stammzertifikats zu einer Server-Vertrauensspeicherdatei auf Seite 148

Das Stammzertifikat für alle vertrauenswürdigen Benutzer muss zu einer Server-Vertrauensspeicherdatei hinzugefügt werden, damit View Connection Server-Instanzen und Sicherheitsserver Smartcard-Benutzer authentifizieren und mit ihren View-Desktops verbinden können.

4 Ändern von View Connection Server-Konfigurationseigenschaften auf Seite 149

Zur Aktivierung der Smartcard-Authentifizierung müssen auf dem View Connection Server- oder Sicherheitsserverhost View Connection Server-Konfigurationseigenschaften geändert werden.

5 Konfigurieren von Smartcard-Einstellungen in View Administrator auf Seite 150

In View Administrator können Einstellungen für verschiedene Smartcard-Authentifizierungsszenarien festgelegt werden.

Anfordern des Stammzertifikats von der Zertifizierungsstelle

Sie müssen das Stammzertifikat von der Zertifizierungsstelle anfordern, welche die Zertifikate auf den von Ihren Benutzern verwendeten Smartcards signiert hat.

Wenn Sie nicht über das Stammzertifikat der Zertifizierungsstelle verfügen, welche die Zertifikate auf den von Ihren Benutzern verwendeten Smartcards signiert hat, können Sie ein Stammzertifikat auch aus einem von einer Zertifizierungsstelle signierten Benutzerzertifikat oder aus einer Smartcard mit Zertifikat exportieren. Siehe „Exportieren eines Stammzertifikats aus einem Benutzerzertifikat“, auf Seite 148.

Vorgehensweise

1 Fordern Sie das Stammzertifikat aus einer der folgenden Quellen an.

- Microsoft IIS-Server, auf dem die Microsoft-Zertifikatdienste ausgeführt werden. Informationen zum Installieren von Microsoft IIS, Ausstellen von Zertifikaten und Verteilen von Zertifikaten in Ihrer Organisation finden Sie auf der Microsoft TechNet-Website.
- Öffentliches Stammzertifikat einer vertrauenswürdigen Zertifizierungsstelle. Dies ist die gängigste Quelle eines Stammzertifikats in Umgebungen, die bereits über eine Smartcard-Infrastruktur und einen standardisierten Ansatz für die Smartcard-Verteilung und -Authentifizierung verfügen.

2 Wählen Sie ein Zertifikat für die Smartcard-Authentifizierung aus.

Die Signaturkette zeigt eine Liste von Zertifizierungsstellen. Typischerweise sollte das Zertifikat der Zwischenzertifizierungsstelle über dem Benutzerzertifikat ausgewählt werden.

3 Stellen Sie sicher, dass die Zertifizierungsstelle keine anderen Zertifikate auf der Smartcard signiert.

Weiter

Fügen Sie das Stammzertifikat zu einer Server-Vertrauensspeicherdatei hinzu. Siehe „Hinzufügen des Stammzertifikats zu einer Server-Vertrauensspeicherdatei“, auf Seite 148.

Exportieren eines Stammzertifikats aus einem Benutzerzertifikat

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Benutzerzertifikat oder eine Smartcard mit Zertifikat verfügen, können Sie das Stammzertifikat exportieren, wenn es von ihrem System als vertrauenswürdig eingestuft wird.

Vorgehensweise

1 Wenn das Benutzerzertifikat auf einer Smartcard vorhanden ist, führen Sie die Smartcard in den Leser ein, um das Benutzerzertifikat zu Ihrem persönlichen Speicher hinzuzufügen.

Wenn das Benutzerzertifikat nicht im persönlichen Speicher angezeigt wird, exportieren Sie das Benutzerzertifikat über die Lesersoftware in eine Datei.

2 Wählen Sie in Internet Explorer **[Tools (Extras)]** > **[Internet Options (Internetoptionen)]** .

3 Klicken Sie auf der Registerkarte **[Content (Inhalte)]** auf **[Certificates (Zertifikate)]** .

4 Wählen Sie auf der Registerkarte **[Personal (Eigene Zertifikate)]** das gewünschte Zertifikat aus und klicken Sie auf **[View (Anzeigen)]** .

Wenn das Benutzerzertifikat nicht in der Liste enthalten ist, klicken Sie auf **[Import (Importieren)]** , um das Zertifikat manuell aus einer Datei zu importieren. Nach dem Import können Sie das Zertifikat aus der Liste auswählen.

5 Wählen Sie auf der Registerkarte **[Certification Path (Zertifizierungspfad)]** das oberste Zertifikat in der Struktur und klicken Sie auf **[View Certificate (Zertifikat anzeigen)]** .

Ein Benutzerzertifikat kann als Bestandteil einer Vertrauenshierarchie signiert werden – das Signaturzertifikat selbst kann durch ein anderes Zertifikat höherer Ebene signiert sein. Wählen Sie das übergeordnete Zertifikat (das Zertifikat, das zum Signieren des Benutzerzertifikats verwendet wurde) als Stammzertifikat aus.

6 Klicken Sie auf der Registerkarte **[Details]** auf **[Copy to File (In Datei kopieren)]** .

Der Zertifikatexport-Assistent wird geöffnet.

7 Klicken Sie auf **[Next (Weiter)]** > **[Next (Weiter)]** und geben Sie einen Namen sowie einen Speicherort für die Exportdatei an.

8 Klicken Sie auf **[Next (Weiter)]** , um die Datei am angegebenen Speicherort als Stammzertifikat zu speichern.

Weiter

Fügen Sie das Stammzertifikat zu einer Server-Vertrauensspeicherdatei hinzu.

Hinzufügen des Stammzertifikats zu einer Server-Vertrauensspeicherdatei

Das Stammzertifikat für alle vertrauenswürdigen Benutzer muss zu einer Server-Vertrauensspeicherdatei hinzugefügt werden, damit View Connection Server-Instanzen und Sicherheitsserver Smartcard-Benutzer authentifizieren und mit ihren View-Desktops verbinden können.

Voraussetzungen

- Fordern Sie das Stammzertifikat von der Zertifizierungsstelle an, welche die Zertifikate auf den von Ihren Benutzern verwendeten Smartcards signiert hat. Siehe „Anfordern des Stammzertifikats von der Zertifizierungsstelle“, auf Seite 147.
- Stellen Sie sicher, dass das Dienstprogramm `keytool` dem Systempfad auf Ihrem View Connection Server- oder Sicherheitsserverhost hinzugefügt wurde. Weitere Informationen finden Sie im Dokument *Installation von VMware View*.

Vorgehensweise

1 Verwenden Sie das Dienstprogramm `keytool` auf Ihren View Connection Server- oder Sicherheitsserverhost, um das Stammzertifikat in die Server-Vertrauensspeicherdatei zu importieren.

Beispiel: **`keytool –import –alias`** ***`Alias`*** **`–file`** ***`Stammzertifikat`*** **`–keystore`** ***`truststorefile.key`***

In diesem Befehl steht *Alias* für einen eindeutigen Namen eines neuen Eintrags in der Vertrauensspeicherdatei (keine Beachtung von Groß-/Kleinschreibung), *Stammzertifikat* gibt das Stammzertifikat an, das Sie angefordert oder exportiert haben, und *truststorefile.key* ist der Name der Vertrauensspeicherdatei, der Sie das Stammzertifikat hinzufügen. Wenn die Datei nicht vorhanden ist, wird sie im aktuellen Verzeichnis erstellt.

HINWEIS Über das Dienstprogramm `keytool` werden Sie möglicherweise zum Erstellen eines Kennworts für die Vertrauensspeicherdatei aufgefordert. Sie werden nach dem Kennwort gefragt, wenn Sie zu einem späteren Zeitpunkt zusätzliche Zertifikate zur Vertrauensspeicherdatei hinzufügen müssen.

2 Kopieren Sie die Vertrauensspeicherdatei in das SSL-Gateway-Konfigurationsverzeichnis auf dem View Connection Server- oder Sicherheitsserverhost.

Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\sslgateway\conf\`*`truststorefile.key`*

Weiter

Ändern Sie die View Connection Server-Konfigurationseigenschaften, um die Smartcard-Authentifizierung zu aktivieren.

Ändern von View Connection Server-Konfigurationseigenschaften

Zur Aktivierung der Smartcard-Authentifizierung müssen auf dem View Connection Server- oder Sicherheitsserverhost View Connection Server-Konfigurationseigenschaften geändert werden.

Voraussetzungen

Fügen Sie das Stammzertifikat für alle vertrauenswürdigen Benutzer zu einer Server-Vertrauensspeicherdatei hinzu.

Vorgehensweise

1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View Connection Server- oder dem Sicherheitsserverhost.

Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Fügen Sie die Eigenschaften `trustKeyfile`, `trustStoretype` und `useCertAuth` zur Datei `locked.properties` hinzu.

a Setzen Sie `trustKeyfile` auf den Namen Ihrer Vertrauensspeicherdatei.

b Setzen Sie `trustStoretype` auf **`JKS`**.

c Setzen Sie `useCertAuth` auf **`true`**, um die Zertifikatauthentifizierung zu aktivieren.

3 Starten Sie den View Connection Server- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: locked.properties-Datei

Mit der gezeigten Datei wird angegeben, dass sich das Stammzertifikat für alle vertrauenswürdigen Benutzer in der Datei `lonqa.key` befindet. Zudem wird der Vertrauensspeichertyp auf JKS gesetzt und die Zertifikatauthentifizierung wird aktiviert.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
```

Weiter

Wenn Sie die Smartcard-Authentifizierung für eine View Connection Server-Instanz konfiguriert haben, konfigurieren Sie die Smartcard-Authentifizierungseinstellungen in View Administrator. Sie müssen die Einstellungen für die Smartcard-Authentifizierung für einen Sicherheitsserver nicht konfigurieren. Bei Sicherheitsservern, die für die Smartcard-Authentifizierung konfiguriert sind, müssen sich Benutzer bei der Anmeldung immer mit einer Smartcard und einer PIN authentifizieren.

Konfigurieren von Smartcard-Einstellungen in View Administrator

In View Administrator können Einstellungen für verschiedene Smartcard-Authentifizierungsszenarien festgelegt werden.

Diese Einstellungen gelten nicht für Sicherheitsserver. Bei Sicherheitsservern, die für die Smartcard-Authentifizierung konfiguriert sind, müssen sich Benutzer bei der Anmeldung immer mit einer Smartcard und einer PIN authentifizieren.

Voraussetzungen

- Ändern Sie View Connection Server-Konfigurationseigenschaften auf Ihrem View Connection Server-Host.
- Stellen Sie sicher, dass in View Administrator in den globalen Einstellungen das Kontrollkästchen **[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]** aktiviert ist. Wenn dieses Kontrollkästchen deaktiviert ist, können keine Smartcard-Authentifizierungsoptionen konfiguriert werden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Server]** .

2 Wählen Sie die gewünschte View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Wählen Sie auf der Registerkarte **[Authentication (Authentifizierung)]** im Dropdown-Menü **[Smart card authentication (Smartcard-Authentifizierung)]** eine Konfigurationsoption aus.

Option	Aufgabe
Not Allowed (Nicht zulässig)	Die Smartcard-Authentifizierung ist auf der View Connection Server-Instanz deaktiviert.
Optional	Benutzer können für die Verbindung mit der View Connection Server-Instanz die Smartcard-Authentifizierung oder die Kennwortauthentifizierung verwenden. Wenn die Smartcard-Authentifizierung fehlschlägt, muss der Benutzer ein Kennwort angeben.
Erforderlich	Benutzer müssen für die Verbindung mit der View Connection Server-Instanz die Smartcard-Authentifizierung verwenden. Wenn die Smartcard-Authentifizierung erforderlich ist, schlägt die Authentifizierung von Benutzern fehl, die das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** zur Herstellung einer Verbindung mit der View Connection Server-Instanz aktivieren. Diese Benutzer müssen sich bei der Anmeldung an View Connection Server erneut mit ihrer Smartcard und ihrer PIN authentifizieren. **Hinweis** Die Smartcard-Authentifizierung ersetzt nur die Windows-Kennwortauthentifizierung. Wenn SecurID aktiviert ist, müssen sich die Benutzer sowohl über SecurID als auch per Smartcard authentifizieren.

4 Konfigurieren Sie die Richtlinie zum Entfernen von Smartcards.

Die Richtlinie zum Entfernen von Smartcards kann nicht konfiguriert werden, wenn für die Smartcard-Authentifizierung **[Not Allowed (Nicht zulässig)]** festgelegt ist.

Option	Aufgabe
Trennen der Benutzer von der View Connection Server-Instanz beim Entfernen der Smartcards	Aktivieren Sie das Kontrollkästchen **[Disconnect user sessions on smart card removal (Benutzersitzungen beim Entfernen von Smartcards trennen)]** .
Benutzer bleiben beim Entfernen der Smartcards weiterhin mit der View Connection Server-Instanz verbunden und können neue Desktop-Sitzungen ohne erneute Authentifizierung starten	Deaktivieren Sie das Kontrollkästchen **[Disconnect user sessions on smart card removal (Benutzersitzungen beim Entfernen von Smartcards trennen)]** .

Die Richtlinie zum Entfernen von Smartcards gilt nicht für Benutzer, die mit der View Connection Server-Instanz verbunden sind, für die das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert ist, selbst wenn sie sich an ihrem Clientsystem mit einer Smartcard anmelden.

Wenn die Richtlinie für Benutzer, die View-Desktops lokal auf ihren Clientsystemen ausführen, zur Trennung von Benutzersitzungen bei Entfernen der Smartcard festgelegt ist, wird das Gastbetriebssystem im View-Desktop bei Entfernen einer Smartcard durch die Benutzer gesperrt. Das View Client-Fenster bleibt geöffnet und Benutzer können **[Optionen] > [Strg-Alt-Entf senden]** auswählen, um sich erneut zu authentifizieren.

5 Klicken Sie auf **[OK]** .

6 Starten Sie den View Connection Server-Dienst neu.

Mit einer Ausnahme müssen Sie den View Connection Server-Dienst neu starten, damit die Änderungen an den Smartcard-Einstellungen in Kraft treten. Sie können bei der Einstellung **[Smart card authentication (Smartcard-Authentifizierung)]** zwischen **[Optional]** und **[Required (Erforderlich)]** wechseln, ohne dabei den View Connection Server-Dienst neu starten zu müssen.

Aktuell angemeldete Benutzer sind von Änderungen an Smartcard-Einstellungen nicht betroffen.

Weiter

Bereiten Sie Active Directory bei Bedarf für die Smartcard-Authentifizierung vor. Siehe „Vorbereiten von Active Directory für die Smartcard-Authentifizierung“, auf Seite 152.

Überprüfen Sie die Konfiguration der Smartcard-Authentifizierung. Siehe „Überprüfen der Smartcard-Authentifizierungskonfiguration“, auf Seite 155.

Vorbereiten von Active Directory für die Smartcard-Authentifizierung

Sie müssen in Active Directory möglicherweise bestimmte Aufgaben ausführen, wenn Sie die Smartcard-Authentifizierung implementieren.

- Hinzufügen von UPNs für Smartcard-Benutzer auf Seite 152

  Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, muss das Active Directory-Konto aller Benutzer, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

- Hinzufügen des Stammzertifikats zum Enterprise NTAuth-Speicher auf Seite 153

  Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

- Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen auf Seite 153

  Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

- Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen auf Seite 154

  Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie **[Intermediate Certification Authorities (Zwischenzertifizierungsstellen)]** in Active Directory hinzufügen.

Hinzufügen von UPNs für Smartcard-Benutzer

Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, muss das Active Directory-Konto aller Benutzer, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, müssen Sie den Benutzer-UPN auf den alternativen Antragstellernamen (Subject Alternative Name, SAN) festlegen, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist. Wenn Ihr Stammzertifikat von einem anderen Server in der aktuellen Domäne des Smartcard-Benutzers ausgegeben wurde, ist eine Änderung des Benutzer-UPNs nicht erforderlich.

Hinweis Sie müssen möglicherweise den UPN für integrierte Active Directory-Konten angeben, selbst wenn das Zertifikat von derselben Domäne ausgegeben wurde. Für integrierte Konten, einschließlich des Administratorkontos, ist standardmäßig kein UPN festgelegt.

Voraussetzungen

- Sie können den alternativen Antragstellernamen (SAN) abrufen, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.

- Wenn das Dienstprogramm „ADSI Edit“ nicht auf Ihrem Active Directory-Server zur Verfügung steht, laden Sie die entsprechenden Windows-Supporttools von der Microsoft-Website herunter und installieren Sie sie.

Vorgehensweise

1 Starten Sie auf Ihrem Active Directory-Server das Dienstprogramm ADSI-Editor.

2 Erweitern Sie im linken Fensterbereich die Domäne, in der sich der Benutzer befindet, und doppelklicken Sie auf `CN=Users`.

3 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Benutzer und anschließend auf **[Properties (Eigenschaften)]** .

4 Doppelklicken Sie auf das Attribut `userPrincipalName` und geben Sie den SAN-Wert für das Zertifikat der vertrauenswürdigen Zertifizierungsstelle ein.

5 Klicken Sie auf **[OK]** , um die Attributeinstellung zu speichern.

Hinzufügen des Stammzertifikats zum Enterprise NTAuth-Speicher

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

- Verwenden Sie auf dem Active Directory-Server den Befehl `certutil`, um das Zertifikat im Enterprise NTAuth-Speicher zu veröffentlichen.

  Beispiel: **`certutil –dspublish –f`** ***`Pfad_zum_Zertifikat_der_Stammzertifizierungsstelle`*** **`NTAuthCA`**

Die Zertifizierungsstelle wird jetzt als vertrauenswürdig eingestuft und kann Zertifikate dieses Typs ausstellen.

Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

1 Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die Domäne und anschließend auf **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie mit der rechten Maustaste auf **[Default Domain Policy (Standarddomänenrichtlinie)]** und anschließend auf **[Edit (Bearbeiten)]** .

5 Erweitern Sie den Abschnitt **[Computer Configuration (Computerkonfiguration)]** und öffnen Sie **[Windows Settings\Security Settings\Public Key Policies (Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel)]** .

6 Klicken Sie mit der rechten Maustaste auf **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** und wählen Sie **[Import (Importieren)]** .

7 Folgen Sie den Anweisungen des Assistenten, um das Stammzertifikat (z.B. `rootCA.cer`) zu importieren. Klicken Sie anschließend auf **[OK]** .

8 Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Stammzertifikats in ihrem vertrauenswürdigen Stammspeicher.

Weiter

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie **[Intermediate Certification Authorities (Zwischenzertifizierungsstellen)]** in Active Directory hinzufügen. Siehe „Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen“, auf Seite 154.

Hinzufügen eines Zwischenzertifikats zu Zwischenzertifizierungsstellen

Wenn Sie eine Zwischenzertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Zwischenzertifikat zur Gruppenrichtlinie **[Intermediate Certification Authorities (Zwischenzertifizierungsstellen)]** in Active Directory hinzufügen.

Vorgehensweise

1 Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die Domäne und anschließend auf **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie mit der rechten Maustaste auf **[Default Domain Policy (Standarddomänenrichtlinie)]** und anschließend auf **[Edit (Bearbeiten)]** .

5 Erweitern Sie den Abschnitt **[Computer Configuration (Computerkonfiguration)]** und öffnen Sie **[Windows Settings\Security Settings\Public Key Policies (Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel)]** .

6 Klicken Sie mit der rechten Maustaste auf **[Intermediate Certification Authorities (Zwischenzertifizierungsstellen)]** und wählen Sie **[Import (Importieren)]** .

7 Folgen Sie den Anweisungen des Assistenten, um das Zwischenzertifikat (z.B. `intermediateCA.cer`) zu importieren. Klicken Sie anschließend auf **[OK]** .

8 Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Zwischenzertifikats in ihrem Zwischenzertifizierungsstellen-Speicher.

Überprüfen der Smartcard-Authentifizierungskonfiguration

Nach der erstmaligen Einrichtung der Smartcard-Authentifizierung oder bei nicht ordnungsgemäßer Funktionsweise der Smartcard-Authentifizierung sollten Sie die Konfiguration der Smartcard-Authentifizierung überprüfen.

Vorgehensweise

- Stellen Sie sicher, dass jedes Clientsystem über View Client, Smartcard-Middleware, eine Smartcard mit gültigem Zertifikat sowie einen Smartcard-Leser verfügt.

  In der Dokumentation Ihres Smartcard-Anbieters finden Sie Informationen zur Konfiguration der Smartcard-Software und -Hardware.

- Wählen Sie auf jedem Clientsystem **[Start] > [Settings (Einstellungen)] > [Control Panel (Systemsteuerung)] > [Internet Options (Internetoptionen)] > [Content (Inhalt)] > [Certificates (Zertifikate)] > [Personal (Eigene Zertifikate)]** um sicherzustellen, dass Zertifikate für die Authentifizierung per Smartcard verfügbar sind.

  Wenn ein Benutzer eine Smartcard in den Smartcard-Leser einlegt, kopiert Windows Zertifikate von der Smartcard für die Verwendung durch View Client auf den Computer des Benutzers.

- Überprüfen Sie in der Datei `locked.properties` auf dem View Connection Server- oder Sicherheitsserverhost, dass die Eigenschaft `useCertAuth` auf **`true`** gesetzt und richtig geschrieben ist.

  Die Datei `locked.properties` befindet sich im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware View\Server\sslgateway\conf`. Die Eigenschaft `useCertAuth` wird durch den Tippfehler `userCertAuth` häufig falsch angegeben.

- Wenn Sie die Smartcard-Authentifizierung auf einer View Connection Server-Instanz konfiguriert haben, überprüfen Sie die Smartcard-Authentifizierungseinstellung im View Administrator.

  a Wählen Sie **[View Configuration (View-Konfiguration)] > [Servers (Server)]** . Wählen Sie die View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .

  b Stellen Sie auf der Registerkarte **[Authentication (Authentifizierung)]** sicher, dass für **[Smart card authentication (Smartcard-Authentifizierung)]** die Einstellung **[Optional]** oder **[Required (Erforderlich)]** festgelegt ist.

  Sie müssen den View Connection Server-Dienst neu starten, damit die Änderungen an den Smartcard-Einstellungen in Kraft treten.

- Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, stellen Sie sicher, dass der Benutzer-UPN auf den alternativen Antragstellernamen (Subject Alternative Name, SAN) festgelegt ist, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist.

  a Sie können den alternativen Antragstellernamen (SAN) ermitteln, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.

  b Wählen Sie auf Ihrem Active Directory-Server **[Start] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

  c Klicken Sie im Ordner **[Users (Benutzer)]** mit der rechten Maustaste auf den Benutzer und wählen Sie **[Properties (Eigenschaften)]** .

  Der Benutzerprinzipalname wird auf der Registerkarte **[Account (Konto)]** in den Textfeldern **[User logon name (Benutzeranmeldename)]** angezeigt.

- Wenn Smartcard-Benutzer für die Verbindung mit View-Desktops das PCoIP-Anzeigeprotokoll verwenden, stellen Sie sicher, dass die Unterfunktion View Agent PCoIP-Smartcard auf den Desktop-Quellen installiert ist. Die Unterfunktion **[PCoIP Smartcard (PCoIP-Smartcard)]** ermöglicht Benutzern die Authentifizierung per Smartcard, wenn sie das PCoIP-Anzeigeprotokoll verwenden.

  HINWEIS Die PCoIP-Smartcard-Unterfunktion wird auf Windows Vista nicht unterstützt.

- Überprüfen Sie auf dem View Connection Server- oder Sicherheitsserverhost die Protokolldateien unter *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs auf Meldungen, die die Aktivierung der Smartcard-Authentifizierung angeben.

Verwenden der Smartcard-Zertifikatssperrüberprüfung

Sie können verhindern, dass sich Benutzer mit gesperrten Benutzerzertifikaten mit Smartcards authentifizieren, indem Sie die Zertifikatssperrüberprüfung konfigurieren. Wenn Benutzer eine Organisation verlassen, eine Smartcard verlieren oder die Abteilung wechseln, werden Zertifikate häufig gesperrt.

View unterstützt die Zertifikatssperrüberprüfung mit Zertifikatssperrlisten und dem Online Certificate Status Protocol (OCSP). Eine Zertifikatssperrliste ist eine Liste mit gesperrten Zertifikaten, die von der Zertifizierungsstelle veröffentlicht wird, die das Zertifikat ausgestellt hat. OCSP ist ein Zertifikatüberprüfungsprotokoll, das zum Abrufen des Sperrstatus eines X.509-Zertifikats verwendet wird.

Die Zertifikatssperrüberprüfung kann auf einer View Connection Server-Instanz oder auf einem Sicherheitsserver konfiguriert werden. Wenn eine View Connection Server-Instanz mit einem Sicherheitsserver kombiniert wird, konfigurieren Sie die Zertifikatssperrüberprüfung auf dem Sicherheitsserver. Der Zugriff auf die Zertifizierungsstelle muss über den View Connection Server- oder Sicherheitsserverhost möglich sein.

Auf einer View Connection Server-Instanz oder einem Sicherheitsserver können sowohl Zertifikatssperrlisten als auch OCSPs verwendet werden. Wenn Sie die Überprüfung mit beiden Zertifikatssperrüberprüfungen konfigurieren, versucht View zunächst, OCSP zu verwenden. Wenn dies nicht möglich ist, wird die Zertifikatssperrliste verwendet. Wenn über die Zertifikatssperrliste keine Überprüfung möglich ist, greift View nicht auf OCSP zurück.

- Anmelden bei Verwendung der Überprüfung von Zertifikatssperrlisten auf Seite 157

  Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, erstellt und liest View eine Zertifikatssperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

- Anmelden bei Verwendung der OCSP-Zertifikatssperrüberprüfung auf Seite 157

  Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. View verwendet ein OCSP-Signaturzertifikat, um die Gültigkeit der vom OCSP-Antwortdienst erhaltenen Antworten zu überprüfen.

- Konfigurieren der Überprüfung von Zertifikatssperrlisten auf Seite 157

  Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, liest View eine Zertifikatssperrliste, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

- Konfigurieren der OCSP-Zertifikatssperrüberprüfung auf Seite 158

  Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View eine Überprüfungsanforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

- Eigenschaften der Smartcard-Zertifikatssperrüberprüfung auf Seite 159

  In der Datei `locked.properties` können Werte zum Aktivieren und Konfigurieren der Smartcard-Zertifikatssperrüberprüfung gesetzt werden.

Anmelden bei Verwendung der Überprüfung von Zertifikatssperrlisten

Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, erstellt und liest View eine Zertifikatssperrliste, um den Sperrstatus eines Benutzerzertifikats zu ermitteln.

Wenn ein Zertifikat gesperrt wird und die Smartcard-Authentifizierung optional ist, wird der Benutzer über das Dialogfeld **[Enter your user name and password (Geben Sie Benutzernamen und Kennwort ein)]** zur Angabe eines Kennworts für die Authentifizierung aufgefordert. Wenn die Smartcard-Authentifizierung erforderlich ist, wird eine Fehlermeldung angezeigt und der Benutzer kann nicht authentifiziert werden. Dasselbe geschieht, wenn View die Zertifikatssperrliste nicht lesen kann.

Anmelden bei Verwendung der OCSP-Zertifikatssperrüberprüfung

Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View eine Anforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines bestimmten Benutzerzertifikats zu ermitteln. View verwendet ein OCSP-Signaturzertifikat, um die Gültigkeit der vom OCSP-Antwortdienst erhaltenen Antworten zu überprüfen.

Wenn das Benutzerzertifikat gesperrt wurde und die Smartcard-Authentifizierung optional ist, wird der Benutzer über das Dialogfeld **[Enter your user name and password (Geben Sie Benutzernamen und Kennwort ein)]** zur Angabe eines Kennworts für die Authentifizierung aufgefordert. Wenn die Smartcard-Authentifizierung erforderlich ist, wird eine Fehlermeldung angezeigt und der Benutzer kann nicht authentifiziert werden.

Wenn View keine oder eine ungültige Antwort vom OCSP-Antwortdienst erhält, wird die Überprüfung von Zertifikatssperrlisten verwendet.

Konfigurieren der Überprüfung von Zertifikatssperrlisten

Wenn Sie die Überprüfung von Zertifikatssperrlisten konfigurieren, liest View eine Zertifikatssperrliste, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

Voraussetzungen

Machen Sie sich mit den Eigenschaften der Datei `locked.properties` für die Überprüfung von Zertifikatssperrlisten vertraut. Siehe „Eigenschaften der Smartcard-Zertifikatssperrüberprüfung“, auf Seite 159.

Vorgehensweise

1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View Connection Server- oder dem Sicherheitsserverhost.

Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Fügen Sie die Eigenschaften `enableRevocationChecking` und `crlLocation` zur Datei `locked.properties` hinzu.

a Setzen Sie `enableRevocationChecking` auf **`true`**, um die Smartcard-Zertifikatssperrüberprüfung zu aktivieren.

b Setzen Sie `crlLocation` auf den Speicherort der Zertifikatssperrliste. Als Wert kann eine URL oder ein Dateipfad angegeben werden.

3 Starten Sie den View Connection Server- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: locked.properties-Datei

Mit der gezeigten Datei wird die Smartcard-Authentifizierung und die Smartcard-Zertifikatssperrüberprüfung aktiviert, die Überprüfung von Zertifikatssperrlisten konfiguriert und eine URL als Speicherort der Zertifikatssperrliste angegeben.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Konfigurieren der OCSP-Zertifikatssperrüberprüfung

Wenn Sie die OCSP-Zertifikatssperrüberprüfung konfigurieren, sendet View eine Überprüfungsanforderung an einen OCSP-Antwortdienst, um den Sperrstatus eines Smartcard-Benutzerzertifikats zu ermitteln.

Voraussetzungen

Machen Sie sich mit den Eigenschaften der Datei `locked.properties` für die OCSP-Zertifikatssperrüberprüfung vertraut. Siehe „Eigenschaften der Smartcard-Zertifikatssperrüberprüfung“, auf Seite 159.

Vorgehensweise

1 Erstellen oder bearbeiten Sie die Datei `locked.properties` im SSL-Gateway-Konfigurationsordner auf dem View Connection Server- oder dem Sicherheitsserverhost.

Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Fügen Sie die Eigenschaften `enableRevocationChecking`, `enableOCSP`, `ocspURL` und `ocspSigningCert` zur Datei `locked.properties` hinzu.

a Setzen Sie `enableRevocationChecking` auf **`true`**, um die Smartcard-Zertifikatssperrüberprüfung zu aktivieren.

b Setzen Sie `enableOCSP` auf **`true`**, um die OCSP-Zertifikatssperrüberprüfung zu aktivieren.

c Setzen Sie `ocspURL` auf die URL des OCSP-Antwortdiensts.

d Setzen Sie `ocspSigningCert` auf den Speicherort der Datei, die das Signaturzertifikat des OCSP-Antwortdiensts enthält.

3 Starten Sie den View Connection Server- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Beispiel: locked.properties-Datei

Mit der gezeigten Datei wird die Smartcard-Authentifizierung und die Smartcard-Zertifikatssperrüberprüfung aktiviert, die Überprüfung von Zertifikatssperrlisten und die OCSP-Zertifikatssperrüberprüfung konfiguriert sowie der Speicherort des OCSP-Antwortdiensts und die Datei mit dem OCSP-Signaturzertifikat angegeben.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Eigenschaften der Smartcard-Zertifikatssperrüberprüfung

In der Datei `locked.properties` können Werte zum Aktivieren und Konfigurieren der Smartcard-Zertifikatssperrüberprüfung gesetzt werden.

Tabelle 7-1 listet die Eigenschaften der Datei `locked.properties` für die Zertifikatssperrüberprüfung auf.

Tabelle 7-1. Eigenschaften für die Smartcard-Zertifikatssperrüberprüfung

Eigenschaft	Beschreibung
`enableRevocationChecking`	Setzen Sie diese Eigenschaft auf **`true`**, um die Zertifikatssperrüberprüfung zu aktivieren. Wenn diese Eigenschaft auf **`false`** gesetzt ist, ist die Zertifikatssperrüberprüfung deaktiviert und alle anderen Eigenschaften für die Zertifikatssperrüberprüfung werden ignoriert. Der Standardwert lautet **`false`**.
`crlLocation`	Gibt den Speicherort der Zertifikatssperrliste als URL oder Dateipfad an. Wenn Sie keine URL angeben oder die angegebene URL nicht gültig ist, verwendet View die Liste der Zertifikatssperrlisten des Benutzerzertifikats, wenn `allowCertCRLs` auf **`true`** gesetzt ist oder nicht angegeben wurde. Wenn View nicht auf eine Zertifikatssperrliste zugreifen kann, schlägt die Überprüfung von Zertifikatssperrlisten fehl.
`allowCertCRLs`	Wenn diese Eigenschaft auf **`true`** gesetzt ist, extrahiert View eine Liste mit Zertifikatssperrlisten aus dem Benutzerzertifikat. Der Standardwert lautet **`true`**.
`enableOCSP`	Setzen Sie diese Eigenschaft auf **`true`**, um die OCSP-Zertifikatssperrüberprüfung zu aktivieren. Der Standardwert lautet **`false`**.
`ocspURL`	Gibt die URL eines OCSP-Antwortdiensts an.
`ocspResponderCert`	Gibt die Datei mit dem Signaturzertifikat des OCSP-Antwortdiensts an. View stellt anhand dieses Zertifikats sicher, dass die Antworten des OCSP-Antwortdiensts gültig sind.
`ocspSendNonce`	Wenn diese Eigenschaft auf **`true`** gesetzt ist, wird mit OCSP-Anforderungen eine Nonce gesendet, um wiederholte Antworten zu verhindern. Der Standardwert lautet **`false`**.
`ocspCRLFailover`	Wenn diese Eigenschaft auf **`true`** gesetzt ist, verwendet View beim Fehlschlagen der OCSP-Zertifikatssperrüberprüfung die Überprüfung von Zertifikatssperrlisten. Der Standardwert lautet **`true`**.

Verwenden der RSA SecurID-Authentifizierung

Eine View Connection Server-Instanz kann so konfiguriert werden, dass sich Benutzer vor der Angabe ihrer Active Directory-Anmeldeinformationen über RSA SecurID authentifizieren müssen.

Da die RSA SecurID-Authentifizierung mit RSA Authentication Manager verwendet wird, ist ein RSA Authentication Manager-Server erforderlich, für den ein direkter Zugriff vom View Connection Server-Host möglich sein muss.

Zur Verwendung der RSA SecurID-Authentifizierung muss jeder Benutzer über ein SecurID-Token verfügen, das für RSA Authentication Manager registriert ist. Bei einem RSA SecurID-Token handelt es sich um Hardware oder Software, über die in festgelegten Intervallen ein Authentifizierungscode generiert wird. Da der Benutzer sowohl eine PIN als auch einen Authentifizierungscode benötigt, bietet RSA SecurID eine zweistufige Authentifizierung. Der Authentifizierungscode ist nur im RSA SecurID-Token verfügbar.

Wenn es mehrere View Connection Server-Instanzen gibt, können Sie die RSA SecurID-Authentifizierung für einige Instanzen konfigurieren und für andere eine andere Benutzerauthentifizierungsmethode einrichten. Sie können beispielsweise die RSA SecurID-Authentifizierung nur für Benutzer konfigurieren, die remote über das Internet auf View-Desktops zugreifen.

VMware View ist gemäß dem RSA SecurID Ready-Programm zertifiziert und unterstützt die vollständige Palette von SecurID-Funktionen, einschließlich New PIN Mode, Next Token Code Mode, RSA Authentication Manager und Lastenausgleich.

- Anmelden bei Verwendung von RSA SecurID auf Seite 160

  Wenn sich ein Benutzer an einer View Connection Server-Instanz anmeldet, für welche die RSA SecurID-Authentifizierung aktiviert wurde, wird in View Client ein RSA SecurID-Anmeldedialogfeld angezeigt.

- Aktivieren der RSA SecurID-Authentifizierung in View Administrator auf Seite 160

  Sie aktivieren eine View Connection Server-Instanz für die RSA SecurID-Authentifizierung, indem Sie die View Connection Server-Einstellungen in View Administrator bearbeiten.

- Fehlerbehebung bei Verweigerung des Zugriffs auf RSA SecurID auf Seite 161

  Bei der Verbindung von View Client mit RSA SecurID-Authentifizierung wird der Zugriff verweigert.

Anmelden bei Verwendung von RSA SecurID

Wenn sich ein Benutzer an einer View Connection Server-Instanz anmeldet, für welche die RSA SecurID-Authentifizierung aktiviert wurde, wird in View Client ein RSA SecurID-Anmeldedialogfeld angezeigt.

Benutzer geben ihren RSA SecurID-Benutzernamen und -Passcode in das RSA SecurID-Anmeldedialogfeld ein. Ein RSA SecurID-Passcode umfasst typischerweise eine PIN, auf die ein Token-Code folgt.

Wenn in RSA Authentication Manager festgelegt ist, dass Benutzer nach der Eingabe von RSA SecurID-Benutzernamen und -Passcode eine neue RSA SecurID-PIN eingeben müssen, wird ein entsprechendes Dialogfeld angezeigt. Nach dem Festlegen einer neuen PIN werden die Benutzer aufgefordert, vor der Anmeldung auf den nächsten Token-Code zu warten. Wenn RSA Authentication Manager für die Verwendung von PINs konfiguriert ist, die vom System generiert werden, wird ein Dialogfeld zur Bestätigung der PIN angezeigt.

Nach einer erfolgreichen Überprüfung gegenüber RSA Authentication Manager werden die Benutzer zur Eingabe ihrer Active Directory-Anmeldeinformationen aufgefordert.

Aktivieren der RSA SecurID-Authentifizierung in View Administrator

Sie aktivieren eine View Connection Server-Instanz für die RSA SecurID-Authentifizierung, indem Sie die View Connection Server-Einstellungen in View Administrator bearbeiten.

Voraussetzungen

- Installieren und Konfigurieren Sie die RSA SecurID-Software.
- Exportieren Sie die Datei `sdconf.rec` für die View Connection Server-Instanz aus RSA Authentication Manager. Weitere Informationen finden Sie in der RSA Authentication Manager-Dokumentation.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Servers (Server)]**.

2 Wählen Sie unter **[View Connection Servers (View Connection Server)]** eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]**.

3 Wählen Sie auf der Registerkarte **[Authentication (Authentifizierung)]** unter **[RSA Secure ID 2-Factor Authentication (Zweistufige RSA SecurID-Authentifizierung)]** die Option **[Enable (Aktivieren)]** .

4 (Optional) Um die Übereinstimmung von RSA SecurID-Benutzernamen und Benutzernamen in Active Directory zu erzwingen, wählen Sie **[Enforce SecurID and Windows user name matching (Übereinstimmung von SecurID- und Windows-Benutzernamen erzwingen)]** .

   Bei Auswahl dieser Option müssen die Benutzer den RSA SecurID-Benutzernamen auch für die Active Directory-Authentifizierung verwenden. Wenn Sie diese Option nicht auswählen, können unterschiedliche Namen gewählt werden.

5 Klicken Sie auf **[Upload File (Datei hochladen)]** und geben Sie den Speicherort der Datei `sdconf.rec` ein oder klicken Sie auf **[Browse (Durchsuchen)]** , um nach der Datei zu suchen.

6 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

   Der View Connection Server-Dienst muss nicht neu gestartet werden. Die erforderlichen Konfigurationsdateien werden automatisch verteilt und die RSA SecurID-Konfiguration wird umgehend angewendet.

Fehlerbehebung bei Verweigerung des Zugriffs auf RSA SecurID

Bei der Verbindung von View Client mit RSA SecurID-Authentifizierung wird der Zugriff verweigert.

Problem

Bei einer View Client-Verbindung mit RSA SecurID wird die Meldung `Access Denied (Zugriff verweigert)` angezeigt und die RSA Authentication Manager-Protokollüberwachung zeigt den Fehler `Node Verification Failed (Knotenverifizierung fehlgeschlagen)` an.

Ursache

Das RSA-Agentenhost-Knotenkennwort muss zurückgesetzt werden.

Lösung

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie unter **[View Connection Servers (View Connection Server)]** die View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Wählen Sie auf der Registerkarte **[Authentication (Authentifizierung)]** die Option **[Clear node secret (Knotenkennwort löschen)]** .

4 Klicken Sie auf **[OK]** , um das Knotenkennwort zu löschen.

5 Wählen Sie auf dem Computer, auf dem RSA Authentication Manager ausgeführt wird, **[Start] > [Programs (Programme)] > [RSA Security (RSA-Sicherheit)] > [RSA Authentication Manager Host Mode (RSA Authentication Manager-Hostmodus)]** .

6 Wählen Sie **[Agent Host (Agentenhost)] > [Edit Agent Host (Agentenhost bearbeiten)]** .

7 Wählen Sie **[View Connection Server]** aus der Liste aus und deaktivieren Sie das Kontrollkästchen **[Node Secret Created (Knotenkennwort erstellt)]** .

   Die Option **[Node Secret Created (Knotenkennwort erstellt)]** wird bei jeder Bearbeitung standardmäßig aktiviert.

8 Klicken Sie auf **[OK]** .

Verwenden der Funktion „Anmelden als aktueller Benutzer“

Wenn View Client-Benutzer das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktivieren, werden die Anmeldeinformationen, die sie bei der Anmeldung am Clientsystem angegeben haben, für die Authentifizierung an der View Connection Server-Instanz und am View-Desktop verwendet. Es ist keine weitere Benutzerauthentifizierung erforderlich.

Zur Unterstützung dieser Funktion werden Anmeldeinformationen sowohl auf der View Connection Server-Instanz als auch auf dem Clientsystem gespeichert.

- Auf der View Connection Server-Instanz werden Anmeldeinformationen verschlüsselt und in der Benutzersitzung zusammen mit dem Benutzernamen, der Domäne und dem optionalen UPN gespeichert. Die Anmeldeinformationen werden hinzugefügt, wenn eine Authentifizierung erfolgt, und gelöscht, wenn das Sitzungsobjekt zerstört wird. Das Sitzungsobjekt wird zerstört, wenn sich der Benutzer abmeldet, das Zeitlimit der Sitzung überschritten wird oder die Authentifizierung fehlschlägt. Das Sitzungsobjekt befindet sich im flüchtigen Speicher und wird nicht in View LDAP oder in einer Datei auf der Festplatte gespeichert.
- Auf dem Clientsystem werden die Anmeldeinformationen von Benutzern verschlüsselt in einer Tabelle im Authentication Package, einer View Client-Komponente, gespeichert. Die Anmeldeinformationen werden der Tabelle hinzugefügt, wenn sich der Benutzer anmeldet, und aus der Tabelle entfernt, wenn er sich abmeldet. Die Tabelle verbleibt im flüchtigen Speicher.

Mit den Gruppenrichtlinieneinstellungen für View Client können Administratoren die Verfügbarkeit des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** steuern und seine Standardeinstellung festlegen. Administratoren können zudem mithilfe der Gruppenrichtlinie die View Connection Server-Instanzen angeben, welche die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** in View Client übergeben werden.

Für die Funktion **[Log in as current user (Anmelden als aktueller Benutzer)]** gelten folgende Einschränkungen und Anforderungen:

- Wird festgelegt, dass die Smartcard-Authentifizierung für eine View Connection Server-Instanz erforderlich ist, müssen sich Smartcard-Benutzer, die das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert haben, weiterhin beim Anmelden an einem View-Desktop mithilfe ihrer Smartcard und PIN erneut authentifizieren.
- Benutzer können einen Desktop nicht zur Verwendung im lokalen Modus auschecken, wenn sie bei der Anmeldung das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert haben.
- Die Uhrzeit auf dem System, an dem sich der Client anmeldet, und die Uhrzeit auf dem View Connection Server-Host müssen synchronisiert werden.
- Wenn die Standardzuweisungen des Benutzerrechts **[Access this computer from the network (Auf diesen Computer vom Netzwerk aus zugreifen)]** auf dem Clientsystem geändert werden, muss diese Änderung wie im VMware Knowledge Base-Artikel 1025691 beschrieben durchgeführt werden.
- Die Client-Maschine muss in der Lage sein, mit dem Active Directory-Unternehmensserver zu kommunizieren, und darf keine zwischengespeicherten Anmeldeinformationen für die Authentifizierung verwenden. Wenn sich Benutzer beispielsweise von außerhalb des Unternehmensnetzwerks bei ihren Client-Maschinen anmelden, werden zwischengespeicherte Anmeldeinformationen für die Authentifizierung verwendet. Wenn der Benutzer dann versucht, eine Verbindung mit einem Sicherheitsserver oder einer Connection Server-Instanz herzustellen, ohne zuerst eine VPN-Verbindung herzustellen, wird der Benutzer aufgefordert, Anmeldeinformationen anzugeben, und die Funktion „Log in as current user (Anmelden als aktueller Benutzer)“ funktioniert nicht.

Konfigurieren von Richtlinien 8

Sie können Richtlinien konfigurieren, um das Verhalten von View-Komponenten, Desktop-Pools und Desktop-Benutzern zu steuern. Mithilfe von View Administrator können Sie Richtlinien für Clientsitzungen festlegen, und Sie können über Active Directory-Gruppenrichtlinieneinstellungen das Verhalten bestimmter View-Funktionen und anderer Funktionen steuern.

Dieses Kapitel behandelt die folgenden Themen:

- „Festlegen von Richtlinien in View Administrator“, auf Seite 163
- „Verwenden von Active Directory-Gruppenrichtlinien“, auf Seite 168
- „Verwenden der Gruppenrichtlinien-ADM-Vorlagendateien für View“, auf Seite 169
- „Einrichten des standortbasierten Drucks“, auf Seite 200
- „Verwenden von Terminaldienste-Gruppenrichtlinien“, auf Seite 204
- „Beispiel einer Active Directory-Gruppenrichtlinie“, auf Seite 205

Festlegen von Richtlinien in View Administrator

Sie können mithilfe von View Administrator Richtlinien für Clientsitzungen konfigurieren.

Sie können diese Richtlinien so festlegen, dass sie auf bestimmte Benutzer, bestimmte Desktop-Pools oder auf alle Clientsitzungsbenutzer angewendet werden. Richtlinien, die für bestimmte Benutzer und Desktop-Pools gelten, werden als Richtlinien auf Benutzer- und Desktop-Ebene bezeichnet. Richtlinien, die sich auf alle Sitzungen und Benutzer auswirken, werden als globale Richtlinien bezeichnet.

Richtlinien auf Benutzerebene erben Einstellungen von äquivalenten Richtlinieneinstellungen für Desktop-Pools. Ähnlich erben Richtlinien auf Pool-Ebene Einstellungen von äquivalenten globalen Richtlinieneinstellungen. Eine Richtlinieneinstellung auf Pool-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung. Eine Richtlinieneinstellung auf Benutzerebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung oder Richtlinieneinstellungen auf Pool-Ebene.

Richtlinieneinstellungen auf einer niedrigeren Ebene können mehr oder weniger restriktiv sein als die äquivalenten Einstellungen höherer Ebene. Wenn beispielsweise die globale Richtlinie zur Festlegung der Auscheckzeit für einen Desktop auf 10 Minuten und die äquivalente Richtlinie auf Pool-Ebene auf 5 Minuten festgelegt ist, können Sie die Richtlinie auf Benutzerebene für beliebige Benutzer im Pool auf 30 Minuten festlegen.

- Konfigurieren globaler Richtlinieneinstellungen auf Seite 164

  Sie können globale Richtlinien konfigurieren, um das Verhalten aller Clientsitzungsbenutzer zu steuern.

- Konfigurieren von Richtlinien für Desktop-Pools auf Seite 164

  Sie können Richtlinien auf Desktop-Ebene konfigurieren, um diese auf spezifische Desktop-Pools anzuwenden. Eine Richtlinieneinstellung auf Desktop-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung.

- Konfigurieren von Richtlinien für Desktop-Benutzer auf Seite 165

  Sie können Richtlinien auf Benutzerebene konfigurieren, um diese auf spezifische Benutzer anzuwenden. Richtlinieneinstellungen auf Benutzerebene haben Vorrang vor äquivalenten globalen Richtlinieneinstellungen und Richtlinieneinstellungen auf Pool-Ebene.

- View-Richtlinien auf Seite 165

  Sie können View-Richtlinien konfigurieren, die auf alle Clientsitzungen angewendet werden, oder Sie wenden die Richtlinien auf spezifische Desktops oder Benutzer an.

- Richtlinien für den lokalen Modus auf Seite 166

  Sie können Richtlinien für den lokalen Modus konfigurieren, die auf alle Clientsitzungen angewendet werden, oder Sie wenden die Richtlinien auf spezifische Desktops oder Benutzer an.

Konfigurieren globaler Richtlinieneinstellungen

Sie können globale Richtlinien konfigurieren, um das Verhalten aller Clientsitzungsbenutzer zu steuern.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Informationen finden Sie in den folgenden Themen:

- „View-Richtlinien“, auf Seite 165
- „Richtlinien für den lokalen Modus“, auf Seite 166

Vorgehensweise

1 Wählen Sie in View Administrator **[Policies (Richtlinien)]** > **[Global Policies (Globale Richtlinien)]** .

   a Zum Konfigurieren allgemeiner Sitzungsrichtlinien klicken Sie im Fensterbereich **[View Policies (View-Richtlinien)]** auf **[Edit policies (Richtlinien bearbeiten)]** .

   b Zum Konfigurieren lokaler Sitzungsrichtlinien klicken Sie im Fensterbereich **[Local Session Policies (Lokale Sitzungsrichtlinien)]** auf **[Edit policies (Richtlinien bearbeiten)]** .

2 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Desktop-Pools

Sie können Richtlinien auf Desktop-Ebene konfigurieren, um diese auf spezifische Desktop-Pools anzuwenden. Eine Richtlinieneinstellung auf Desktop-Ebene hat Vorrang vor einer äquivalenten globalen Richtlinieneinstellung.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Informationen finden Sie in den folgenden Themen:

- „View-Richtlinien“, auf Seite 165
- „Richtlinien für den lokalen Modus“, auf Seite 166

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **[Policies (Richtlinien)]** .

Die Registerkarte **[Policies (Richtlinien)]** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **[Pool Policy (Pool-Richtlinie)]** der Wert **[Inherit (Vererben)]** angezeigt.

3 Zum Konfigurieren allgemeiner Sitzungsrichtlinien für den Pool klicken Sie im Fensterbereich **[View Policies (View-Richtlinien)]** auf **[Edit policies (Richtlinien bearbeiten)]** .

4 Zum Konfigurieren lokaler Sitzungsrichtlinien für den Pool klicken Sie im Fensterbereich **[Local Mode Policies (Richtlinien für den lokalen Modus)]** auf **[Edit policies (Richtlinien bearbeiten)]** .

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Konfigurieren von Richtlinien für Desktop-Benutzer

Sie können Richtlinien auf Benutzerebene konfigurieren, um diese auf spezifische Benutzer anzuwenden. Richtlinieneinstellungen auf Benutzerebene haben Vorrang vor äquivalenten globalen Richtlinieneinstellungen und Richtlinieneinstellungen auf Pool-Ebene.

Voraussetzungen

Machen Sie sich mit den Richtlinienbeschreibungen vertraut. Siehe „View-Richtlinien“, auf Seite 165.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [Pools]** .

2 Doppelklicken Sie auf die ID des Desktop-Pools und anschließend auf die Registerkarte **[Policies (Richtlinien)]** .

Die Registerkarte **[Policies (Richtlinien)]** zeigt die aktuellen Richtlinieneinstellungen. Wenn eine Einstellung von der äquivalenten globalen Richtlinie vererbt wird, wird in der Spalte **[Pool Policy (Pool-Richtlinie)]** der Wert **[Inherit (Vererben)]** angezeigt.

3 Klicken Sie auf **[User Overrides (Außerkraftsetzungen durch Benutzer)]** und anschließend auf **[Add user (Benutzer hinzufügen)]** .

4 Um einen Benutzer zu suchen, klicken Sie auf **[Add (Hinzufügen)]** , geben den Namen oder die Beschreibung des Benutzers ein und klicken anschließend auf **[Find (Suchen)]** .

5 Wählen Sie einen oder mehrere Benutzer aus der Liste aus, klicken Sie auf **[OK]** und anschließend auf **[Next (Weiter)]** .

Das Dialogfeld **[Add Individual Policy (Einzelne Richtlinie hinzufügen)]** wird angezeigt.

6 Allgemeine Sitzungsrichtlinien konfigurieren Sie auf der Registerkarte **[General (Allgemein)]** .

7 Richtlinien für Clients im lokalen Modus können auf der Registerkarte **[Local (Lokal)]** konfiguriert werden.

8 Klicken Sie auf **[Finish (Fertig stellen)]** , um Ihre Änderungen zu speichern.

View-Richtlinien

Sie können View-Richtlinien konfigurieren, die auf alle Clientsitzungen angewendet werden, oder Sie wenden die Richtlinien auf spezifische Desktops oder Benutzer an.

Tabelle 8-1 beschreibt alle View-Richtlinieneinstellungen.

Tabelle 8-1. View-Richtlinien

Richtlinie	Beschreibung
Multimedia redirection (MMR)	Legt fest, ob MMR für Clientsysteme aktiviert ist. MMR ist ein Microsoft DirectShow-Filter, der Multimediadaten von bestimmten Codecs auf View-Desktops direkt über einen TCP-Socket an das Clientsystem weiterleitet. Die Daten werden direkt auf dem Clientsystem decodiert, auf dem sie wiedergegeben werden. Der Standardwert lautet **[Allow (Zulassen)]** . Wenn Clientsysteme über unzureichende Ressourcen zum Verarbeiten der lokalen Multimedia-Decodierung verfügen, ändern Sie die Einstellung in **[Deny (Ablehnen)]** . MMR arbeitet nicht ordnungsgemäß, wenn die Hardware zur Videoanzeige auf dem Clientsystem keine Overlay-Unterstützung bietet.
USB Access (USB-Zugriff)	Legt fest, ob Desktops USB-Geräte verwenden können, die mit dem Clientsystem verbunden sind. Der Standardwert lautet **[Allow (Zulassen)]** . Um aus Sicherheitsgründen die Verwendung externer Geräte zu unterbinden, ändern Sie die Einstellung in **[Deny (Ablehnen)]** .
Remote mode (Remote-Modus)	Legt fest, ob Benutzer sich mit Desktops verbinden und verwenden können, die auf vCenter Server-Instanzen ausgeführt werden. Ist diese Einstellung auf **[Deny (Ablehnen)]** festgelegt, müssen Benutzer den Desktop auf ihren lokalen Computern auschecken und können den Desktop nur im lokalen Modus ausführen. Die Beschränkung der Benutzer auf die ausschließliche Ausführung von Desktops im lokalen Modus senkt die Kosten in Bezug auf CPU- und Arbeitsspeicherressourcen sowie die benötigte Netzwerkbandbreite zur Ausführung des Desktops auf einem Back-End-Server. Der Standardwert lautet **[Allow (Zulassen)]** .
PCoIP hardware acceleration (PCoIP-Hardwarebeschleunigung)	Legt fest, ob die Hardwarebeschleunigung für das PCoIP-Anzeigeprotokoll aktiviert wird und legt die Beschleunigungspriorität fest, die der PCoIP-Benutzersitzung zugewiesen ist. Diese Einstellung hat nur dann Auswirkungen, wenn ein PCoIP-Hardwarebeschleunigungsgerät auf dem physischen Computer vorhanden ist, der den Desktop hostet. Der Standardwert lautet **[Allow (Zulassen)]** , mit dem Prioritätswert **[Medium (Mittel)]** .

Richtlinien für den lokalen Modus

Sie können Richtlinien für den lokalen Modus konfigurieren, die auf alle Clientsitzungen angewendet werden, oder Sie wenden die Richtlinien auf spezifische Desktops oder Benutzer an.

Tabelle 8-2 beschreibt alle Richtlinieneinstellungen für den lokalen Modus.

Tabelle 8-2. Richtlinien für den lokalen Modus

Richtlinie	Beschreibung
Local Mode (Lokaler Modus)	Legt fest, ob Benutzer ihre Desktops für die lokale Verwendung auschecken können. Legt außerdem fest, ob Benutzer lokale Desktops ausführen können, wenn die Desktops ausgecheckt sind. Der Standardwert lautet **[Allow (Zulassen)]** . Wenn Sie diesen Wert in **[Deny (Ablehnen)]** ändern, während ein Desktop ausgecheckt ist, kann der Benutzer den Desktop nicht im lokalen Modus ausführen, und der Desktop kann nicht remote verwendet werden, da er noch ausgecheckt ist.
User-initiated Rollback (Benutzer-initiiertes Rollback)	Legt fest, ob Benutzer einen lokalen Desktop verwerfen und auf die Remote-Version zurücksetzen können. Wenn ein Benutzer den Rollback-Vorgang initiiert, wird die Sperre für den Remote-Desktop aufgehoben und der lokale Desktop wird verworfen. Falls erforderlich, kann der Benutzer den lokalen Ordner, der die Daten zum lokalen Desktop enthält, manuell entfernen. Der Standardwert lautet **[Allow (Zulassen)]** .
Max time without server contact (Maximale Zeit ohne Serverkontakt)	Gibt die Dauer in Tagen an, die ein lokaler Desktop ausgeführt werden kann, ohne dass zum Abruf von Richtlinienaktualisierungen eine Verbindung mit View Connection Server hergestellt werden muss. Wenn das angegebene Zeitlimit überschritten wurde, zeigt View Client dem Benutzer eine Warnmeldung an und hält den Desktop an. Der Standardwert lautet **7** Tage. Clientseitig wird diese Ablaufrichtlinie in einer Datei gespeichert, die mit einem in der Anwendung integrierten Schlüssel verschlüsselt wird. Mit diesem integrierten Schlüssel wird verhindert, dass Benutzer mit Zugriff auf das Kennwort die Ablaufrichtlinie umgehen.
Target replication frequency (Zielreplikationshäufigkeit)	Über diese Einstellung wird das Intervall in Tagen, Stunden oder Minuten zwischen dem Start einer Replikation und dem Start der nächsten Replikation angegeben. Bei einer Replikation werden alle Änderungen an lokalen Desktop-Dateien in die entsprechenden Remote-Desktops oder auf eine persistente View Composer-Festplatte im Rechenzentrum kopiert. Die Standardeinstellung lautet **[No replication (Keine Replikation)]** . Wenn Sie die Einstellung **[At a specified interval (Im angegebenen Intervall)]** auswählen, beträgt das Standardintervall für die Replikation 12 Stunden. Bei Auswahl von **[No replication (Keine Replikation)]** sind keine geplanten Replikationen zulässig. Durch die Richtlinie **[No replication (Keine Replikation)]** werden explizite Replikationsanforderungen nicht verhindert. Wenn die Richtlinie **[User initiated replication (Vom Benutzer initiierte Replikation)]** auf **[Allow (Zulassen)]** gesetzt ist, können Sie Replikationen in View Administrator initiieren und Benutzer können Replikationen anfordern. Wenn eine Replikation länger dauert als das in der Richtlinie **[Target replication frequency (Zielreplikationshäufigkeit)]** angegebene Intervall, wird die nächste geplante Replikation gestartet, sobald die vorherige Replikation abgeschlossen ist. Die vorherige Replikation wird durch die ausstehende Replikation nicht beendet. Beispiel: In der Richtlinie **[Target replication frequency (Zielreplikationshäufigkeit)]** ist als Intervall ein Tag festgelegt. Eine Replikation kann beispielsweise um 12:00 Uhr am Dienstag beginnen. Wenn der Clientcomputer vom Netzwerk getrennt ist, kann die Replikation länger als 24 Stunden in Anspruch nehmen. Am Mittwoch um 12:00 Uhr startet View Client with Local Mode die nächste Replikationsanforderung. Nach Abschluss der vorherigen Replikation erstellt View Client with Local Mode einen Snapshot und startet die ausstehende Replikation.

Tabelle 8-2. Richtlinien für den lokalen Modus (Fortsetzung)

Richtlinie	Beschreibung
User deferred replication (Vom Benutzer verzögerte Replikation)	Legt fest, ob Benutzer aktive Replikationen anhalten können. Wenn Sie diese Richtlinie aktivieren, kann ein Benutzer eine laufende Replikation verschieben. Die Replikation wird nicht fortgesetzt und neue Replikationen werden erst nach Ablauf des Verzögerungszeitraums gestartet. Der Standardwert lautet **[Deny (Ablehnen)]** . Wenn Sie den Wert **[Allow (Zulassen)]** auswählen, wird der Verzögerungszeitraum auf zwei Stunden festgelegt.
Disks replicated (Festplattenreplikation)	Legt fest, welche Desktop-Festplatten repliziert werden. Diese Richtlinie gilt nur für View Composer-Linked-Clone-Desktops. Bei Desktops auf Grundlage vollständiger virtueller Maschinen werden alle Festplatten repliziert. Bei der Festplattenreplikation stehen die folgenden Optionen zur Auswahl: ■ Persistente Festplatten ■ Betriebssystemfestplatten ■ OS and persistent disks (Betriebssystem- und persistente Festplatten) Eine Änderung dieser Richtlinie wirkt sich auf die Desktop-Replikation nach dem nächsten Auschecken aus. Eine Änderung wirkt sich nicht auf derzeit ausgecheckte Desktops aus. Der Standardwert lautet **[Persistent disks (Persistente Festplatten)]** .
User initiated check in (Vom Benutzer initiiertes Einchecken)	Legt fest, ob Benutzer Desktops einchecken dürfen, die im lokalen Modus ausgeführt werden. Der Standardwert lautet **[Allow (Zulassen)]** .
User initiated replication (Vom Benutzer initiierte Replikation)	Legt fest, ob Benutzer von ihren Desktops aus Replikationen initiieren dürfen, wenn die Desktops im lokalen Modus ausgeführt werden. Der Standardwert lautet **[Allow (Zulassen)]** .

Verwenden von Active Directory-Gruppenrichtlinien

Sie können Microsoft Windows-Gruppenrichtlinien dazu verwenden, Ihre View-Desktops zu optimieren und zu schützen, das Verhalten der View-Komponenten zu steuern und den standortbasierten Druck zu konfigurieren.

Gruppenrichtlinien sind eine Funktion der Microsoft Windows-Betriebssysteme, die eine zentrale Verwaltung und Konfiguration von Computern und Remote-Benutzern in einer Active Directory-Umgebung ermöglichen.

Gruppenrichtlinieneinstellungen sind in Entitäten enthalten, die als GPOs (Group Policy Objects, Gruppenrichtlinienobjekte) bezeichnet werden. GPOs sind mit Active Directory-Objekten verknüpft. GPOs können auf Domänenebene auf View-Komponenten angewendet werden, um verschiedene Bereiche der View-Umgebung zu steuern. Nach der Aktivierung von GPOs werden GPO-Einstellungen in der lokalen Windows-Registrierung der betreffenden Komponente gespeichert.

Zur Verwaltung von Gruppenrichtlinieneinstellungen verwenden Sie den Gruppenrichtlinienobjekt-Editor von Microsoft Windows. Der Gruppenrichtlinienobjekt-Editor ist ein MMC-Snap-In (Microsoft Management Console). Die MMC ist Bestandteil der Gruppenrichtlinien-Verwaltungskonsole von Microsoft. Informationen zu Installation und Verwendung der Gruppenrichtlinien-Verwaltungskonsole finden Sie auf der Microsoft TechNet-Website.

Erstellen einer OU für View-Desktops

Sie sollten in Active Directory eine Organisationseinheit (Organizational Unit, OU) erstellen, die speziell für Ihre View-Desktops verwendet wird.

Um zu verhindern, dass Gruppenrichtlinieneinstellungen auf andere Windows-Server oder -Arbeitsstationen in derselben Domäne wie Ihre Desktops angewendet werden, erstellen Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für Ihre View Manager-Gruppenrichtlinien und verknüpfen es mit der OU, die Ihre View-Desktops enthält.

Informationen zum Erstellen von OUs und GPOs finden Sie in der Microsoft Active Directory-Dokumentation auf der Microsoft TechNet-Website.

Aktivieren der Loopback-Verarbeitung für View-Desktops

Standardmäßig stammen die Richtlinieneinstellungen für einen Benutzer aus einem Satz an Gruppenrichtlinienobjekten (Group Policy Objects, GPOs), die in Active Directory auf das Benutzerobjekt angewendet werden. In der View-Umgebung jedoch sollten GPOs basierend auf dem Computer angewendet werden, an dem sich der Benutzer anmeldet.

Wenn Sie die Loopback-Verarbeitung aktivieren, wird ein konsistenter Richtliniensatz auf alle Benutzer angewendet, die sich an einem bestimmten Computer anmelden – unabhängig von ihrer Position in Active Directory.

Informationen zum Aktivieren der Loopback-Verarbeitung finden Sie in der Dokumentation zu Microsoft Active Directory.

HINWEIS Die Loopback-Verarbeitung ist nur ein Ansatz bei der Verarbeitung von GPOs in View. Sie müssen möglicherweise einen anderen Ansatz implementieren.

Verwenden der Gruppenrichtlinien-ADM-Vorlagendateien für View

View umfasst verschiedene komponentenspezifische administrative Vorlagendateien für Gruppenrichtlinien (ADM-Vorlagendateien). Sie können View-Desktops optimieren und schützen, indem Sie die Richtlinieneinstellungen in diesen ADM-Vorlagendateien zu einem neuen oder vorhandenen Gruppenrichtlinienobjekt (Group Policy Object, GPO) in Active Directory hinzufügen.

Die View-ADM-Vorlagendateien enthalten sowohl Gruppenrichtlinien für die Computerkonfiguration als auch Gruppenrichtlinien für die Benutzerkonfiguration.

- Richtlinien für die Computerkonfiguration gelten für alle View-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.
- Richtlinien für die Benutzerkonfiguration gelten für alle Benutzer, unabhängig davon, mit welchem View-Desktop sie sich verbinden. Richtlinien für die Benutzerkonfiguration setzen gleichwertige Richtlinien für die Computerkonfiguration außer Kraft.

View wendet Richtlinien beim Start eines View-Desktops und bei der Benutzeranmeldung an.

ADM-Vorlagendateien für View

Die View-ADM-Vorlagendateien werden im Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\extras\GroupPolicyFiles auf Ihrem View Connection Server-Host installiert.

Tabelle 8-3. ADM-Vorlagendateien für View

Name der Vorlage	Vorlagendatei	Beschreibung
VMware View Agent-Konfiguration	vdm_agent.adm	Enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung sowie Umgebungskomponenten von View Agent.
VMware View Client-Konfiguration	vdm_client.adm	Enthält Richtlinieneinstellungen in Bezug auf die View Client-Konfiguration. Auf Clients, die von außerhalb der View Connection Server-Hostdomäne eine Verbindung herstellen, wirken sich die auf View Client angewendeten Richtlinien nicht aus.
VMware View Server-Konfiguration	vdm_server.adm	Enthält Richtlinieneinstellungen in Bezug auf View Connection Server.
Allgemeine VMware View-Konfiguration	vdm_common.adm	Enthält Richtlinieneinstellungen, die für alle View-Komponenten gelten.
VMware View PCoIP-Sitzungsvariablen	pcoip.adm	Enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll.
VMware View Persona-Verwaltung-Konfiguration	ViewPM.adm	Enthält Richtlinieneinstellungen in Bezug auf View Persona-Verwaltung. Siehe „Gruppenrichtlinieneinstellungen für View Persona-Verwaltung“, auf Seite 223.

ADM-Vorlageneinstellungen für die View Agent-Konfiguration

Die ADM-Vorlagendatei (vdm_agent.adm) für die View Agent-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die Authentifizierung und die Umgebungskomponenten von View Agent.

Tabelle 8-4 werden alle Richtlinieneinstellungen in der ADM-Vorlagendatei für die View Agent-Konfiguration beschrieben. Die Vorlage enthält sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 8-4. Vorlageneinstellungen für die View Agent-Konfiguration

Einstellung	Computer	Benutzer	Eigenschaften
`AllowDirectRDP (Direkte RDP-Verbindung zulassen)`	X		Legt fest, ob Nicht-View Clients über RDP eine direkte Verbindung mit View-Desktops herstellen können. Ist diese Einstellung deaktiviert, lässt View Agent nur View-verwaltete Verbindungen über View Client zu. Wenn Sie die Verbindung zu einem virtuellen Desktop über View Client für Mac OS X herstellen, deaktivieren Sie nicht die Einstellung `AllowDirectRDP (Direkte RDP-Verbindung zulassen)`. Wenn diese Einstellung deaktiviert ist, schlägt die Verbindungsherstellung mit einem Fehler vom Typ `Access is denied (Zugriff verweigert)` fehl. Diese Einstellung ist standardmäßig aktiviert.
`AllowSingleSignon (Einmalige Anmeldung (Single Sign-On) zulassen)`	X		Legt fest, ob zur Verbindungsherstellung mit View-Desktops die einmalige Anmeldung (Single Sign-On, SSO) zulässig ist. Bei Aktivierung dieser Einstellung werden Benutzer nur dann zur Eingabe ihrer Anmeldeinformationen aufgefordert, wenn Sie eine Verbindung mit View Client herstellen. Ist diese Einstellung deaktiviert, müssen sich die Benutzer beim Herstellen einer Remote-Verbindung erneut authentifizieren. Diese Einstellung ist standardmäßig aktiviert.
`CommandsToRunOnConnect (Befehle, die beim Verbinden auszuführen sind)`	X		Gibt eine Liste mit Befehlen oder Befehlsskripts an, die bei der ersten Verbindungsherstellung ausgeführt werden. Siehe „Ausführen von Befehlen auf View-Desktops“, auf Seite 172 .
`CommandsToRunOnReconnect (Befehle, die beim Verbinden auszuführen sind)`	X		Gibt eine Liste mit Befehlen oder Befehlsskripts an, die ausgeführt werden, wenn eine Sitzung nach einer Verbindungstrennung wiederhergestellt wird. Siehe „Ausführen von Befehlen auf View-Desktops“, auf Seite 172 .
`Connect Using DNS Name (Beim Verbinden DNS-Namen verwenden)`	X		Legt fest, ob View Connection Server beim Herstellen der Verbindung anstelle der IP-Adresse des Hosts den DNS-Namen verwendet. Diese Einstellung ist häufig in einer NAT- oder Firewall-Umgebung aktiviert, wenn View Client oder View Connection Server die IP-Adresse des Desktops nicht direkt verwenden kann. Diese Einstellung ist standardmäßig deaktiviert.
`ConnectionTicketTimeout (Verbindungsticket abgelaufen)`	X		Gibt die Gültigkeitsdauer des View-Verbindungstickets in Sekunden an. View-Clients verwenden bei der Verbindungsherstellung mit View Agent zur Überprüfung und für die einmalige Anmeldung ein Verbindungsticket. Ein Verbindungsticket ist aus Sicherheitsgründen nur für einen begrenzten Zeitraum gültig. Wenn ein Benutzer eine Verbindung zu einem View-Desktop herstellt, muss die Authentifizierung innerhalb des Gültigkeitszeitraums des Verbindungstickets erfolgen, ansonsten wird die Sitzung aufgrund einer Zeitüberschreitung beendet. Wenn diese Einstellung nicht konfiguriert ist, beträgt die standardmäßige Dauer bis zur Zeitüberschreitung 900 Sekunden.
`CredentialFilterExceptions (CredentialFilter-Ausnahmen)`	X		Gibt die ausführbaren Dateien an, die nicht zum Laden des CredentialFilter-Agenten berechtigt sind. Dateinamen dürfen weder einen Pfad noch ein Suffix enthalten. Verwenden Sie ein Semikolon zum Trennen mehrerer Dateinamen.

Tabelle 8-4. Vorlageneinstellungen für die View Agent-Konfiguration (Fortsetzung)

Einstellung	Computer	Benutzer	Eigenschaften
Disable Time Zone Synchronization (Zeitzonensynchronisation deaktivieren)	X	X	Legt fest, ob die Zeitzone des View-Desktops mit der des verbundenen Clients synchronisiert wird. Diese Einstellung wird bei Aktivierung nur angewendet, wenn die Einstellung Disable Time Zone Forwarding der Richtlinie für die View Client-Konfiguration nicht auf **[Disabled (Deaktiviert)]** gesetzt wurde. Diese Einstellung ist standardmäßig deaktiviert.
Force MMR to use software overlay (MMR zwingen, ein Software-Overlay zu verwenden)	X		Legt fest, ob die MMR-Funktion (Multimedia Redirection) anstelle eines Hardware-Overlays ein Software-Overlay verwendet. Zur Optimierung der Leistung verwendet MMR Videoanzeige-Hardware mit Overlay-Unterstützung. Da Hardware-Overlays bei einem Multi-Monitor-System im Allgemeinen nur auf dem primären Monitor verwendet werden, funktioniert die Videoanzeige nicht, wenn sie vom primären Monitor auf einen sekundären Monitor gezogen wird. Durch Aktivierung dieser Einstellung wird MMR gezwungen, ein Software-Overlay auf allen Monitoren zu verwenden. Diese Einstellung ist standardmäßig deaktiviert.
ShowDiskActivityIcon (Desktop-Activity-Icon anzeigen)	X		Diese Einstellung wird in der vorliegenden Version nicht unterstützt.
Toggle Display Settings Control (Display-Einstellungen ein- und ausschalten)	X		Legt fest, ob in der Systemsteuerung unter **[Display (Anzeige)]** die Registerkarte **[Settings (Einstellungen)]** deaktiviert ist, wenn eine Clientsitzung das PCoIP-Anzeigeprotokoll verwendet. Diese Einstellung ist standardmäßig aktiviert.

Ausführen von Befehlen auf View-Desktops

Sie können die View Agent-Gruppenrichtlinieneinstellungen CommandsToRunOnConnect und CommandsToRunOnReconnect dazu verwenden, um Befehle und Befehlsskripts auf View-Desktops auszuführen, wenn sich Benutzer verbinden oder erneut verbinden.

Um einen Befehl oder ein Befehlsskript auszuführen, fügen Sie den Befehlsnamen oder den Dateipfad des Skripts zur Liste der Befehle für die Gruppenrichtlinieneinstellung hinzu. Beispiel:

```
date
```

```
C:\Scripts\myscript.cmd
```

Um Skripts auszuführen, die einen Konsolenzugriff erfordern, stellen Sie die Option -C oder -c voran, gefolgt von einem Leerzeichen. Beispiel:

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

Zu den unterstützten Dateitypen gehören .CMD, .BAT und .EXE. .VBS-Dateien werden erst nach einer Analyse mit cscript.exe oder wscript.exe ausgeführt. Beispiel:

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

Die Gesamtlänge der Zeichenfolge, einschließlich der Option -C oder -c, darf 260 Zeichen nicht überschreiten.

An View-Desktops gesendete Clientsysteminformationen

Wenn Benutzer sich mit einem View-Desktop verbinden oder erneut verbinden, ruft der View-Client Informationen zum Clientsystem ab und View Connection Server sendet diese Informationen an den Desktop. View Agent schreibt die Clientcomputerinformationen in den Systemregistrierungspfad `HKCU\Volatile Environment` auf dem Desktop.

Sie können den View Agent-Gruppenrichtlinieneinstellungen `CommandsToRunOnConnect` und `CommandsToRunOnReconnect` Befehle hinzufügen, um Befehle oder Befehlsskripts auszuführen, die diese Informationen aus der Systemregistrierung lesen, wenn sich Benutzer mit Desktops verbinden oder erneut verbinden. Weitere Informationen finden Sie unter „Ausführen von Befehlen auf View-Desktops“, auf Seite 172.

Tabelle 8-5 beschreibt die Registrierungsschlüssel, die Clientsysteminformationen enthalten, und listet die Arten von Clientsystemen auf, die diese unterstützen.

Tabelle 8-5. Clientsysteminformationen

Registrierungsschlüssel	Beschreibung	Unterstützte Clientsysteme
`ViewClient_IP_Address`	Die IP-Adresse des Clientsystems.	Windows Linux Mac
`ViewClient_MAC_Address`	Die MAC-Adresse des Clientsystems.	Windows Linux Mac
`ViewClient_Machine_Name`	Der Computername des Clientsystems.	Windows Linux Mac
`ViewClient_Machine_Domain`	Die Domäne des Clientsystems.	Windows Linux Mac
`ViewClient_LoggedOn_Username`	Der Benutzername, der zur Anmeldung am Clientsystem verwendet wurde.	Windows Linux Mac
`ViewClient_LoggedOn_Domainname`	Der Domänenname, der zur Anmeldung am Clientsystem verwendet wurde.	Windows **Hinweis** Informationen zu Linux- und Mac-Clients finden Sie unter `ViewClient_Machine_Domain`. `ViewClient_LoggedOn_Domainname` wird vom Linux- bzw. Mac-Client nicht bereitgestellt, da Linux- bzw. Mac-Konten nicht an Windows-Domänen gebunden sind.
`ViewClient_Type`	Der Thin Client-Name oder Betriebssystemtyp des Clientsystems.	Windows Linux Mac
`ViewClient_Broker_DNS_Name`	Der DNS-Name der View Connection Server-Instanz.	Windows Linux Mac
`ViewClient_Broker_URL`	Die URL der View Connection Server-Instanz.	Windows Linux Mac

Tabelle 8-5. Clientsysteminformationen (Fortsetzung)

Registrierungsschlüssel	Beschreibung	Unterstützte Clientsysteme
`ViewClient_Broker_Tunneled`	Der Status der Tunnelverbindung für View Connection Server, der entweder `true` (aktiviert) oder `false` (deaktiviert) lauten kann.	Windows Linux Mac
`ViewClient_Broker_Tunnel_URL`	Die URL der View Connection Server-Tunnelverbindung, wenn die Tunnelverbindung aktiviert ist.	Windows Linux Mac
`ViewClient_Broker_Remote_IP_Address`	Die IP-Adresse der View Connection Server-Instanz, mit der der Client verbunden ist.	Windows Linux Mac
`ViewClient_TZID`	Die Olson-Zeitzonen-ID. Zum Deaktivieren der Zeitzonensynchronisierung aktivieren Sie die View Agent-Gruppenrichtlinieneinstellung `Disable Time Zone Synchronization`.	Linux Mac

ADM-Vorlageneinstellungen für die View Client-Konfiguration

Die ADM-Vorlagendatei (`vdm_client.adm`) für die View Client-Konfiguration enthält Richtlinieneinstellungen in Bezug auf die View Client-Konfiguration.

Einstellungen für die Skriptdefinition

Tabelle 8-6 werden die Einstellungen für die Skriptdefinition in der ADM-Vorlagendatei für die View Client-Konfiguration beschrieben. Die Vorlage stellt für jede Skriptdefinition eine Version für die Computerkonfiguration und eine Version für die Benutzerkonfiguration bereit. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 8-6. View Client-Konfigurationsvorlage: Skriptdefinitionen

Einstellung	Beschreibung
`Connect all USB devices to the desktop on launch (Alle USB-Geräte mit dem Desktop verbinden, wenn dieser gestartet wird)`	Legt fest, ob alle der verfügbaren USB-Geräte auf dem Clientsystem mit dem Desktop verbunden werden, wenn dieser gestartet wird.
`Connect all USB devices to the desktop when they are plugged in (Alle USB-Geräte mit dem Desktop verbinden, wenn diese angeschlossen werden)`	Legt fest, ob USB-Geräte mit dem Desktop verbunden werden, wenn die Geräte an das Clientsystem angeschlossen werden.
`DesktopLayout (erfordert DesktopName)`	Legt das Layout des View Client-Fensters fest, das einem Benutzer bei der Anmeldung an einem View-Desktop angezeigt wird. Es stehen folgende Optionen zur Auswahl: ■ `Full Screen (Vollbildmodus)` ■ `Mehrere Monitore` ■ `Fenster - Groß` ■ `Fenster - Klein` Diese Einstellung ist nur verfügbar, wenn die Einstellung `DesktopName to select (DesktopName auswählen)` ebenfalls gesetzt ist.
`DesktopName to select (DesktopName auswählen)`	Legt den von View Client während der Anmeldung verwendeten Standard-Desktop fest.

Tabelle 8-6. View Client-Konfigurationsvorlage: Skriptdefinitionen (Fortsetzung)

Einstellung	Beschreibung
`Disable 3rd-party Terminal Services plugins (Terminaldienste-Plug-Ins von Drittanbietern deaktivieren)`	Legt fest, ob Terminaldienste-Plug-Ins von Drittanbietern, die als normale RDP-Plug-Ins installiert sind, von View Client überprüft werden. Wenn Sie diese Einstellung nicht konfigurieren, überprüft View Client standardmäßig Plug-Ins von Drittanbietern. Diese Einstellung hat keine Auswirkung auf View-spezifische Plug-Ins, wie beispielsweise die USB-Umleitung.
`Logon DomainName (DomainName für Anmeldung)`	Legt die von View Client während der Anmeldung verwendete NetBIOS-Domäne fest.
`Logon Password (Passwort für Anmeldung)`	Legt das von View Client während der Anmeldung verwendete Kennwort fest. Das Kennwort wird von Active Directory im Textformat gespeichert.
`Logon UserName (UserName für Anmeldung)`	Legt den von View Client während der Anmeldung verwendeten Benutzernamen fest.
`Server URL`	Legt die von View Client während der Anmeldung verwendete URL fest, z. B. `http://view1.beispiel.com`.
`Suppress error messages (nur bei Skriptverwendung)`	Legt fest, ob View Client Fehlermeldungen während der Anmeldung unterdrückt. Diese Einstellung ist nur anwendbar, wenn der Anmeldevorgang vollständig per Skript ausgeführt wird, z.B. wenn alle erforderlichen Anmeldeinformationen über eine Richtlinie vorausgefüllt werden. Wenn die Anmeldung aufgrund von falschen Anmeldeinformationen fehlschlägt, wird der Benutzer hierüber nicht benachrichtigt, und der View Client-Prozess `wswc.exe` wird beendet.

Sicherheitseinstellungen

Tabelle 8-7 werden die Sicherheitseinstellungen in der ADM-Vorlagendatei für die View Client-Konfiguration beschrieben. Diese Tabelle zeigt, ob die Einstellungen die Einstellungen „Computer Configuration (Computerkonfiguration)“ und User Configuration (Benutzerkonfiguration)“ enthalten oder nur die Einstellung „Computer Configuration (Computerkonfiguration)“. Bei den Sicherheitseinstellungen, die beide Typen einschließen, setzt die Einstellung für die Benutzerkonfiguration hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 8-7. View Client-Konfigurationsvorlage: Sicherheitseinstellungen

Einstellung	Computer	Benutzer	Beschreibung
`Allow command line credentials (Anmeldeinformationen von der Befehlszeile ausführen)`	X		Legt fest, ob Benutzeranmeldeinformationen mit View Client-Befehlszeilenoptionen bereitgestellt werden können. Wenn diese Einstellung aktiviert ist, stehen die Optionen `smartCardPIN` und `password` nicht zur Verfügung, wenn Benutzer View Client von der Befehlszeile ausführen. Diese Einstellung ist standardmäßig aktiviert.
`Brokers Trusted For Delegation`	X		Gibt die View Connection Server-Instanzen an, welche die Benutzeridentitäts- und Anmeldeinformationen akzeptieren, die bei Aktivierung des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** übergeben werden. Wenn Sie keine View Connection Server-Instanzen angeben, akzeptieren alle View Connection Server-Instanzen diese Informationen. Verwenden Sie zum Hinzufügen einer View Connection Server-Instanz eines der folgenden Formate: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Service Principal Name (SPN) des View Connection Server-Dienstes

Tabelle 8-7. View Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Certificate verification mode (Zertifikatüberprüfungsmodus)`	X		Konfiguriert die Ebene der Zertifikatüberprüfung, die durch View Client durchgeführt wird. Es stehen folgende Modi zur Auswahl: ■ `No Security (Keine Sicherheit)`. View führt keine Überprüfung durch. ■ `Warn But Allow (Warnen, aber zulassen)`. Wenn die folgenden Serverzertifikatprobleme auftreten, wird eine Warnung angezeigt, aber der Benutzer kann mit der Verbindungsherstellung mit View Connection Server fortfahren: ■ Von View wird ein selbstsigniertes Zertifikat bereitgestellt. In diesem Fall ist es akzeptabel, wenn der Zertifikatname nicht mit dem Namen des View Connection Servers übereinstimmt, der in View Client vom Benutzer angegeben wurde. ■ Ein überprüfbares Zertifikat, das in Ihrer Bereitstellung konfiguriert wurde, ist abgelaufen oder noch nicht gültig.

Tabelle 8-7. View Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
			Wenn andere Zertifikatfehlerbedingungen vorliegen, zeigt View ein Fehlerdialogfeld an und verhindert, dass der Benutzer eine Verbindung mit View Connection Server herstellt. `Warn But Allow (Warnen, aber zulassen)` ist der Standardwert. ■ `Full Security (Volle Sicherheit)`. Wenn ein beliebiger Zertifikatfehler auftritt, kann der Benutzer keine Verbindung mit View Connection Server herstellen. View zeigt dem Benutzer die Zertifikatfehler an. Damit View Client das Zertifikat überhaupt überprüft, müssen Sie die globale Einstellung **[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]** in View Administrator auswählen. Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, können die Benutzer den ausgewählten Modus für die Zertifikatüberprüfung in View Client sehen, ihn aber nicht konfigurieren. Das Dialogfeld für die SSL-Konfiguration informiert die Benutzer darüber, dass der Administrator die Einstellung gesperrt hat. Wenn diese Einstellung nicht konfiguriert oder deaktiviert wurde, können View Client-Benutzer SSL konfigurieren und einen Modus für die Zertifikatüberprüfung auswählen. Wenn Sie diese Einstellung bei Windows-Clients nicht als Gruppenrichtlinie konfigurieren möchten, können Sie die Zertifikatüberprüfung auch durch Hinzufügen des Wertnamens `CertCheckMode` zum folgenden Registrierungsschlüssel auf dem Clientcomputer aktivieren: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` Verwenden Sie die folgenden Werte im Registrierungsschlüssel: ■ **`0`** implementiert `No Security (Keine Sicherheit)`. ■ **`1`** implementiert `Warn But Allow (Warnen, aber zulassen)`. ■ **`2`** implementiert `Full Security (Volle Sicherheit)`. Wenn Sie sowohl die Gruppenrichtlinieneinstellung als auch die Einstellung `CertCheckMode` im Registrierungsschlüssel konfigurieren, hat die Gruppenrichtlinieneinstellung Vorrang vor der Registrierungsschlüsseleinstellung.

Tabelle 8-7. View Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Default value of the 'Log in as current user' checkbox (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer')`	X	X	Gibt den Standardwert des Kontrollkästchens **[Log in as current user (Anmelden als aktueller Benutzer)]** im Dialogfeld für die View Client-Verbindung an. Diese Einstellung setzt den Standardwert außer Kraft, der während der View Client-Installation angegeben wurde. Wenn ein Benutzer View Client von der Befehlszeile ausführt und die Option `logInAsCurrentUser` angibt, überschreibt der eingegebene Wert diese Einstellung. Wenn das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** aktiviert ist, werden die Identität und die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem verwendet, an die View Connection Server-Instanz und schließlich an den View-Desktop übergeben. Ist das Kontrollkästchen deaktiviert, müssen Benutzer Identitäts- und Anmeldeinformationen mehrere Male eingeben, bevor Sie auf einen View-Desktop zugreifen können. Diese Einstellung ist standardmäßig deaktiviert.
`Display option to Log in as current user (Option zum Anmelden als aktueller Benutzer anzeigen)`	X	X	Legt fest, ob das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** im Dialogfeld für die View Client-Verbindung angezeigt wird. Bei Anzeige des Kontrollkästchens können Benutzer die Option aktivieren oder deaktivieren oder den zugehörigen Standardwert außer Kraft setzen. Wird das Kontrollkästchen ausgeblendet, können Benutzer den Standardwert im Dialogfeld für die View Client-Verbindung nicht ändern. Sie können den Standardwert für **[Log in as current user (Anmelden als aktueller Benutzer)]** über die Richtlinieneinstellung `Default value of the 'Log in as current user' checkbox (Standardwert des Kontrollkästchens 'Anmelden als aktueller Benutzer')` festlegen. Diese Einstellung ist standardmäßig aktiviert.
`Enable jump list integration (Integration der Sprungliste aktivieren)`	X		Legt fest, ob eine Sprungliste im View Client-Symbol in der Taskleiste von Windows 7 oder höheren Systemen angezeigt werden soll. Über die Sprungliste können sich Benutzer mit zuletzt verwendeten View Connection Server-Instanzen und View-Desktops verbinden. Wenn View Client gemeinsam verwendet wird, können Benutzern die Namen zuletzt verwendeter Desktops angezeigt werden. Die Sprungliste können Sie deaktivieren, indem Sie diese Einstellung deaktivieren. Diese Einstellung ist standardmäßig aktiviert.
`Enable Single Sign-On for smart card authentication (Aktivieren von Single Sign-On für die Smartcard-Authentifizierung)`	X		Legt fest, ob für die Smartcard-Authentifizierung das Single Sign-On (SSO) aktiviert ist. Ist SSO aktiviert, speichert View Client die verschlüsselte Smartcard-PIN im temporären Arbeitsspeicher, bevor sie an View Connection Server gesendet wird. Ist SSO deaktiviert, zeigt View Client kein benutzerdefiniertes PIN-Dialogfeld an.

Tabelle 8-7. View Client-Konfigurationsvorlage: Sicherheitseinstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
Ignore bad SSL certificate date received from the server (Vom Server erhaltenes SSL Zertifikat mit ungültigen Datumswerten ignorieren)	X		Legt fest, ob Fehler in Zusammenhang mit ungültigen Datumswerten für das Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn ein Server ein abgelaufenes Zertifikat sendet. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore certificate revocation problems (Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignorieren)	X		Legt fest, ob Fehler in Zusammenhang mit einem gesperrten Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der Server ein Zertifikat sendet, das gesperrt wurde, und der Client den Sperrstatus eines Zertifikats nicht überprüfen kann. Diese Einstellung ist standardmäßig deaktiviert. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore incorrect SSL certificate common name (host name field) (Fehler in Zusammenhang mit falschen allgemeinen Namen im SSL-Zertifikat ignorieren)	X		Legt fest, ob Fehler in Zusammenhang mit falschen allgemeinen Namen im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn der allgemeine Name des Zertifikats nicht mit dem Hostnamen des Servers übereinstimmt, der das Zertifikat sendet. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore incorrect usage problems (Fehler in Zusammenhang mit einer falschen Verwendung ignorieren)	X		Legt fest, ob Fehler in Zusammenhang mit einer falschen Verwendung des Serverzertifikats ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat für einen anderen Zweck als die Überprüfung der Absenderidentität und zum Verschlüsseln der Serverkommunikation gedacht ist. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
Ignore unknown certificate authority problems (Fehler in Zusammenhang mit einer unbekannten Zertifizierungsstelle ignorieren)	X		Legt fest, ob bestimmte Fehler in Zusammenhang mit einer unbekannten Zertifizierungsstelle im Serverzertifikat ignoriert werden. Diese Fehler treten auf, wenn das vom Server gesendete Zertifikat durch eine nicht vertrauenswürdige Drittanbieter-Zertifizierungsstelle signiert wurde. Diese Einstellung gilt nur für View 4.6 und frühere Releases.

RDP-Einstellungen

Tabelle 8-8 werden die RDP-Einstellungen (Remote Desktop Protocol) in der ADM-Vorlagendatei für die View Client-Konfiguration beschrieben. Alle RDP-Einstellungen sind Einstellungen für die Benutzerkonfiguration.

Tabelle 8-8. ADM-Vorlage für View Client-Konfiguration: RDP-Einstellungen

Einstellung	Beschreibung
`Audio redirection (Umleiten von Audio)`	Legt fest, ob auf dem View-Desktop wiedergegebene Audioinformationen umgeleitet werden. Es stehen folgende Einstellungen zur Auswahl: **Disable Audio** – Die Audiowiedergabe ist deaktiviert. **Play VM (erforderlich für VoIP USB-Unterstützung)** – Audiodaten werden im View-Desktop wiedergegeben. Diese Einstellung erfordert ein gemeinsam genutztes USB-Audiogerät zur Wiedergabe von Sound auf dem Client. **Redirect to client** – Audiodaten werden an den Client umgeleitet. Dies ist der Standardmodus. Diese Eigenschaft gilt nur für RDP-Audio. Über MMR umgeleitete Audiodaten werden im Client wiedergegeben.
`Audio capture redirection (Umleitung der Audioaufnahme)`	Legt fest, ob das standardmäßige Audioeingabegerät vom Client an die Remote-Sitzung umgeleitet wird. Wenn diese Einstellung aktiviert ist, wird das Audioaufzeichnungsgerät des Clients im View-Desktop angezeigt und kann zur Aufzeichnung von Audioeingabedaten verwendet werden. Diese Einstellung ist standardmäßig deaktiviert.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps (Bitmap-Cache-Dateigröße in Einheit für Anzahl der bbp-Bitmaps)`	Gibt die Größe des Bitmapcaches (in KB oder MB) für die Zwischenspeicherung von Bitmaps mit einer bestimmten Farbeinstellung (Bits pro Pixel, bpp) an. Für die verschiedenen Kombinationen aus Einheit und Bits pro Pixel stehen unterschiedliche Versionen zur Verfügung: ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`Bitmap caching (Bitmap zwischenspeichern)`	Legt fest, ob Remote-Bitmaps auf dem lokalen Computer zwischengespeichert werden.
`Cache persistence active (Dauerhafte Zwischenspeicherung aktiv)`	Legt fest, ob für Bitmaps eine dauerhafte Zwischenspeicherung durchgeführt wird (aktiv ist). Eine dauerhafte Zwischenspeicherung für Bitmaps kann die Leistung verbessern, erfordert jedoch zusätzlichen Speicherplatz.
`Color Depth (Farbtiefe)`	Legt die Farbtiefe für den View-Desktop fest. Es stehen folgende Einstellungen zur Auswahl: ■ 8 Bit ■ 15 Bit ■ 16 Bit ■ 24 Bit ■ 32 Bit Für Windows XP-Systeme mit 24 Bit müssen Sie die Richtlinie Limit Maximum Color Depth in **[Computer Configuration (Computerkonfiguration)] > [Administrative Templates (Administrative Vorlagen)] > [Windows Components (Windows-Komponenten)] > [Terminaldienste]** aktivieren und auf 24 Bit festlegen.
`Cursor shadow (Cursor-Schattierung)`	Legt fest, ob auf dem View-Desktop unter dem Cursor ein Schatten angezeigt wird.
`Desktop Background (Desktop-Hintergrund)`	Legt fest, ob der Desktop-Hintergrund angezeigt wird, wenn sich Clients mit einem View-Desktop verbinden.

Tabelle 8-8. ADM-Vorlage für View Client-Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
`Desktop composition (Desktop-Gestaltung)`	(Windows Vista oder höher) Legt fest, ob die Desktop-Gestaltung auf dem View-Desktop aktiviert ist. Wenn die Desktop-Gestaltung aktiviert ist, werden einzelne Fenster nicht länger direkt auf dem Bildschirm oder dem primären Anzeigegerät dargestellt, wie dies in früheren Versionen von Microsoft Windows der Fall war. Stattdessen werden die Bilddaten zunächst in den nicht sichtbaren Offscreen-Bereich des Videospeichers umgeleitet und anschließend zur Darstellung auf dem Anzeigegerät in ein Desktop-Bild gerendert.
`Enable compression (Komprimieren aktivieren)`	Legt fest, ob RDP-Daten komprimiert werden. Diese Einstellung ist standardmäßig aktiviert.
`Enable Credential Security Service Provider (Dienstanbieter für Sicherung der Benutzeranmeldedaten aktivieren)`	Gibt an, ob die View-Desktop-Verbindung NLA (Network Level Authentication) verwendet. In Windows Vista erfordern Remote-Desktop-Verbindungen standardmäßig NLA. Wenn das Gastbetriebssystem für Remote-Desktop-Verbindungen NLA erfordert, müssen Sie diese Einstellung aktivieren. Andernfalls kann View Client keine Verbindung zum View-Desktop herstellen. Zusätzlich zur Aktivierung dieser Einstellung müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind: ■ Sowohl das Client- als auch das Gastbetriebssystem unterstützen NLA. ■ Für die View Connection Server-Instanz sind direkte Clientverbindungen aktiviert. Tunnelverbindungen werden mit NLA nicht unterstützt.
`Enable RDP Auto-Reconnect (automatische erneute RDP-Verbindung aktivieren)`	Legt fest, ob die RDP-Clientkomponente versucht, erneut eine Verbindung mit einem View-Desktop herzustellen, nachdem ein RDP-Verbindungsfehler aufgetreten ist. Diese Einstellung hat keine Auswirkung, wenn die Einstellung **[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]** in View Administrator aktiviert ist. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Die automatische erneute RDP-Verbindung wird für Desktops mit View Agent 4.5 oder einer höheren Version unterstützt. Wenn ein Desktop eine frühere Version von View Agent verwendet, können einige Funktionen nicht verwendet werden.
`Font smoothing (Schriftglättung)`	(Windows Vista oder höher) Legt fest, ob ein Anti-Aliasing auf die Schriftarten auf dem View-Desktop angewendet wird.
`Menu and window animation (Menü- und Fensteranimation)`	Legt fest, ob die Animation für Menüs und Fenster aktiviert ist, wenn sich Clients mit einem View-Desktop verbinden.
`Redirect clipboard (Zwischenablage umleiten)`	Legt fest, ob die Informationen in der lokalen Zwischenablage umgeleitet werden, wenn sich Clients mit dem View-Desktop verbinden.
`Redirect drives (Treiber umleiten)`	Legt fest, ob lokale Festplattenlaufwerke umgeleitet werden, wenn Clients sich mit dem View-Desktop verbinden. Lokale Laufwerke werden standardmäßig umgeleitet. Durch Aktivieren oder Nichtkonfigurieren dieser Einstellung können Daten auf dem umgeleiteten Laufwerk des Remote-Desktops auf das Laufwerk des Clientcomputers kopiert werden. Deaktivieren Sie diese Einstellung, wenn das Übertragen von Daten vom Remote-Desktop zu den Clientcomputern des Benutzers ein mögliches Sicherheitsrisiko für Ihre Bereitstellung darstellt. Alternativ können Sie auch die Ordnerumleitung in der virtuellen Maschine des Remote-Desktops deaktivieren, indem Sie die Microsoft Windows-Gruppenrichtlinieneinstellung `Do not allow drive redirection (Laufwerkumleitung nicht zulassen)` aktivieren. Die Einstellung `Redirect drives (Laufwerke umleiten)` wirkt sich nur auf RDP aus.

Tabelle 8-8. ADM-Vorlage für View Client-Konfiguration: RDP-Einstellungen (Fortsetzung)

Einstellung	Beschreibung
Redirect printers (Drucker umleiten)	Legt fest, ob lokale Drucker umgeleitet werden, wenn Clients sich mit dem View-Desktop verbinden.
Redirect serial ports (Serielle Ports umleiten)	Legt fest, ob lokale COM-Ports umgeleitet werden, wenn Clients sich mit dem View-Desktop verbinden.
Redirect smart cards (Smartcards umleiten)	Legt fest, ob lokale Smartcards umgeleitet werden, wenn Clients sich mit dem View-Desktop verbinden. **Hinweis** Diese Einstellung gilt sowohl für RDP- als auch für PCoIP-Verbindungen.
Redirect supported plug-and-play devices (Unterstützte Plug-and-Play-Geräte umleiten)	Legt fest, ob lokale Plug & Play- sowie POS-Geräte (Point of Sale) umgeleitet werden, wenn Clients sich mit dem View-Desktop verbinden. Dieses Verhalten unterscheidet sich dahingehend von der Umleitung, dass es durch die View Agent-Komponente für die USB-Umleitung verwaltet wird.
Shadow bitmaps (Schattenbitmaps)	Legt fest, ob Schattenbitmaps verwendet werden. Diese Einstellung hat im Vollbildmodus keine Auswirkung.
Show contents of window while dragging (Inhalte anzeigen, wenn diese an einen neuen Ort gezogen werden)	Legt fest, ob Ordnerinhalte angezeigt werden, wenn der Benutzer einen Ordner an einen neuen Speicherort zieht.
Themes (Themen)	Legt fest, ob Designs angezeigt werden, wenn sich Clients mit einem View-Desktop verbinden.
Windows key combination redirection (Umleiten von Windows-Tastenkombinationen)	Legt fest, ob Windows-Tastenkombinationen angewendet werden.

Allgemeine Einstellungen

Tabelle 8-9 werden die allgemeinen Einstellungen in der ADM-Vorlagendatei für die View Client-Konfiguration beschrieben. Zu den allgemeinen Einstellungen gehören sowohl Einstellungen für die Computerkonfiguration als auch Einstellungen für die Benutzerkonfiguration. Die Einstellung für die Benutzerkonfiguration setzt hierbei die äquivalente Einstellung für die Computerkonfiguration außer Kraft.

Tabelle 8-9. View Client-Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Computer	Benutzer	Beschreibung
Always on top (Immer im Vordergrund)		X	Legt fest, ob das View Client-Fenster immer im Vordergrund angezeigt wird. Durch Aktivierung dieser Einstellung wird verhindert, dass die Windows-Taskleiste ein View Client-Fenster im Vollbildmodus überlappt. Diese Einstellung ist standardmäßig aktiviert.
Default Exit Behavior For Local Mode Desktops (Standardverhalten beim Beenden von Desktops, die im lokalen Modus ausgeführt werden)		X	Steuert das Standardverhalten beim Beenden von Desktops, die im lokalen Modus ausgeführt werden. Die Standardeinstellung lautet **[Shutdown (Herunterfahren)]** , bei der das Gastbetriebssystem heruntergefahren wird.

Tabelle 8-9. View Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
`Delay the start of replications when starting the View Client with Local Mode (Starten von Replikationen nach dem Start von View Client with Local Mode verzögern.)`	X		Gibt die Verzögerungszeit in Sekunden an, mit der die Replikation nach dem Start von View Client with Local Mode gestartet wird. Bei einer Replikation werden alle Änderungen an Dateien des lokalen Desktops in den entsprechenden Remote-Desktop kopiert. Die nächste geplante Replikation beginnt nach dem Verzögerungszeitraum. Replikationsvorgänge werden in bestimmten Intervallen ausgeführt, die in den Richtlinien für den lokalen Modus in View Administrator angegeben werden. Die Standardverzögerung beträgt 900 Sekunden (15 Minuten).
`Determines if the VMware View Client should use proxy.pac file (Legt fest, ob der VMware View Client eine proxy.pac-Datei verwenden soll)`	X		Legt fest, ob View Client eine PAC-Datei (Proxy Automatic Configuration) verwendet. Wenn diese Einstellung aktiviert ist, verwendet View Client eine PAC-Datei. Eine PAC-Datei (häufig als `proxy.pac` bezeichnet) hilft Webbrowsern und anderen Agenten, den geeigneten Proxy-Server für eine bestimmte URL oder Website-Anforderung zu finden. Wenn Sie diese Einstellung auf einer Maschine mit mehreren Kernen aktivieren, stürzt möglicherweise die WinINet-Anwendung ab, die View Client für die Suche nach Proxy-Server-Informationen verwendet. Deaktivieren Sie diese Einstellung, wenn dieses Problem auf Ihrer Maschine auftritt. Diese Einstellung ist standardmäßig deaktiviert. **Hinweis** Diese Einstellung gilt nur für direkte Verbindungen. Auf Tunnelverbindungen hat die Einstellung keine Auswirkung. Diese Einstellung gilt nur für View 4.6 und frühere Releases.
`Disable Time Zone Forwarding (Zeitzonenweiterleitung deaktivieren)`	X		Legt fest, ob die Zeitzonensynchronisierung des View-Desktops mit der des verbundenen Clients deaktiviert ist.
`Disable toast notifications (Toastnachrichten deaktivieren)`			Hierdurch wird festgelegt, ob Toastnachrichten von View Client deaktiviert werden sollen. Aktivieren Sie diese Einstellung, wenn Sie nicht möchten, dass dem Benutzer Toastnachrichten in der Ecke des Bildschirms angezeigt werden. **Hinweis** Wenn Sie diese Einstellung aktivieren, wird dem Benutzer bei Aktivierung der Funktion „Sitzungszeitüberschreitung“ keine 5-Minuten-Warnung eingeblendet.
`Don't check monitor alignment on spanning (Monitoranordnung beim Spanning nicht überprüfen)`		X	Standardmäßig wird der Client-Desktop nicht in den Mehrfachmonitor-Modus geschaltet, wenn die Bildschirme in Kombination kein exaktes Rechteck bilden (d.h. identische Höhe bei horizontaler Anordnung oder identische Breite bei vertikaler Anordnung). Aktivieren Sie diese Einstellung, um den Standardwert außer Kraft zu setzen. Diese Einstellung ist standardmäßig deaktiviert.

Tabelle 8-9. View Client-Konfigurationsvorlage: Allgemeine Einstellungen (Fortsetzung)

Einstellung	Computer	Benutzer	Beschreibung
Enable multi-media acceleration (Multimedia-Beschleunigung aktivieren)		X	Legt fest, ob die Multimedia-Umleitung (Multimedia Redirection, MMR) auf dem Client aktiviert ist. MMR arbeitet nicht ordnungsgemäß, wenn die View Client-Hardware zur Videoanzeige keine Overlay-Unterstützung bietet. Die MMR-Richtlinie gilt nicht für lokale Desktop-Sitzungen.
Enable the shade (Schatten aktivieren)		X	Legt fest, ob die Schatten-Menüleiste im oberen Bereich des View Client-Fensters sichtbar ist. Diese Einstellung ist standardmäßig aktiviert. **Hinweis** Die Schatten-Menüleiste im oberen Bereich ist für den Kiosk-Modus standardmäßig deaktiviert.
Redirect smart card readers in Local Mode (Smartcard-Leser in Local Mode umleiten)	X		Legt fest, ob Smartcard-Leser an lokale Desktops umgeleitet werden. Die Leser werden gemeinsam mit dem Clientsystem genutzt. Diese Einstellung ist standardmäßig aktiviert.
Tunnel proxy bypass address list (Adressenliste um Tunnel und Proxy zu umgehen.)	X		Gibt eine Liste von Tunneladressen an. Der Proxy-Server wird für diese Adressen nicht verwendet. Verwenden Sie ein Semikolon (;) zum Trennen mehrerer Einträge.
URL for View Client online help (URL für View Client Hilfeseiten)	X		Gibt eine alternative URL an, von der View Client Hilfeseiten abrufen kann. Diese Einstellung ist zur Verwendung in Umgebungen gedacht, die das remote verwaltete Hilfesystem nicht abrufen können, da kein Internetzugriff verfügbar ist.
Pin the Shade (Menüleiste fixieren)		X	Legt fest, ob die Fixierung der Menüleiste im oberen Bereich des View Client-Fensters aktiviert ist, sodass die Menüleiste nicht automatisch ausgeblendet wird. Diese Einstellung hat keine Auswirkung, wenn die Menüleiste deaktiviert wurde. Diese Einstellung ist standardmäßig aktiviert.

ADM-Vorlageneinstellungen für die View Server-Konfiguration

Die ADM-Vorlagendatei (`vdm_server.adm`) für die View Server-Konfiguration enthält Richtlinieneinstellungen in Bezug auf alle View Connection Server-Instanzen.

Tabelle 8-10 beschreibt die in der ADM-Vorlagendatei für die View Server-Konfiguration enthaltenen Richtlinieneinstellungen. Die Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

Tabelle 8-10. Vorlageneinstellungen für die View Server-Konfiguration

Einstellung	Eigenschaften
`Recursive Enumeration of Trusted Domains`	Legt fest, ob alle Domänen aufgelistet werden, die von der Serverdomäne als vertrauenswürdig eingestuft werden. Um eine vollständige Vertrauenskette zu erzielen, werden rekursiv auch die vertrauten Domänen aller vertrauten Domänen aufgelistet – so lange, bis alle vertrauten Domänen ermittelt wurden. Diese Informationen werden an View Connection Server weitergeleitet um sicherzustellen, dass für die Clientanmeldung alle vertrauten Domänen verfügbar sind. Diese Einstellung ist standardmäßig aktiviert. Ist diese Einstellung deaktiviert, werden nur Domänen mit einem direkten Vertrauensverhältnis aufgelistet, eine Verbindung mit Remote-Domänencontrollern findet nicht statt. In Umgebungen mit komplexen Domänenbeziehungen – z.B. in Umgebungen mit mehreren Gesamtstrukturen, bei denen Vertrauensstellungen zwischen den Domänen der Gesamtstrukturen eingerichtet wurden – kann dieser Vorgang mehrere Minuten in Anspruch nehmen.

ADM-Vorlageneinstellungen für die allgemeine View-Konfiguration

Die ADM-Vorlagendatei (`vdm_common.adm`) für die allgemeine View Server-Konfiguration enthält Richtlinieneinstellungen, die für alle View-Komponenten gelten. Diese Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

Einstellungen für die Protokollkonfiguration

Tabelle 8-11 beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen Richtlinieneinstellungen für die Protokollkonfiguration.

Tabelle 8-11. Allgemeine View-Konfigurationsvorlage: Einstellungen für die Protokollkonfiguration

Einstellung	Eigenschaften
`Number of days to keep production logs`	Gibt an, für wie lange (in Tagen) Protokolldateien auf dem System gespeichert werden. Wenn kein Wert festgelegt ist, gilt die Standardeinstellung, nach der Protokolldateien für 7 Tage beibehalten werden.
`Maximum number of debug logs`	Gibt an, wie viele Debug-Protokolldateien maximal auf dem System gespeichert werden. Wenn eine Protokolldatei ihre maximale Größe erreicht, werden keine weiteren Einträge hinzugefügt, und es wird eine neue Protokolldatei erstellt. Wenn die Anzahl der vorherigen Protokolldateien den hier angegebenen Wert erreicht, wird die älteste Protokolldatei gelöscht.
`Maximum debug log size in Megabytes`	Gibt die maximale Größe in Megabyte an, die eine Debug-Protokolldatei erreichen darf, bevor die Protokolldatei geschlossen und eine neue Protokolldatei erstellt wird.
`Log Directory`	Gibt den vollständigen Pfad zum Verzeichnis für Protokolldateien an. Wenn für den Speicherort kein Schreibzugriff möglich ist, wird der standardmäßige Speicherort verwendet. Für Clientprotokolldateien wird ein gesondertes Verzeichnis mit dem Namen des Clients erstellt.

Einstellungen für Leistungsalarme

Tabelle 8-12 beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen Einstellungen für Leistungsalarme.

Tabelle 8-12. Allgemeine View-Konfigurationsvorlage: Einstellungen für Leistungsalarme

Einstellung	Eigenschaften
`CPU and Memory Sampling Interval in Seconds`	Gibt das Abrufintervall für CPU und Arbeitsspeicher an. Ein niedriges Samplingintervall kann zu einer großen Menge an Ausgabedaten im Protokoll führen.
`Overall CPU usage percentage to issue log info`	Gibt den Schwellenwert an, bei dem die CPU-Gesamtnutzung des Systems protokolliert wird. Wenn mehrere Prozessoren verfügbar sind, gibt der Prozentwert die kombinierte Nutzung an.
`Overall memory usage percentage to issue log info`	Gibt den Schwellenwert an, bei dem die Gesamtnutzung des zugesicherten Systemarbeitsspeichers protokolliert wird. Zugesicherter Systemarbeitsspeicher ist der Arbeitsspeicher, der von Prozessoren reserviert wurde und für den das Betriebssystem physischen Arbeitsspeicher oder Platz in der Auslagerungsdatei zugesichert hat.
`Process CPU usage percentage to issue log info`	Gibt den Schwellenwert an, bei dem die CPU-Nutzung einzelner Prozesse protokolliert wird.
`Process memory usage percentage to issue log info`	Gibt den Schwellenwert an, bei dem die Arbeitsspeichernutzung einzelner Prozesse protokolliert wird.
`Process to check, comma separated name list allowing wild cards and exclusion`	Gibt eine kommagetrennte Liste mit Abfragen an, die dem Namen von einem oder mehreren Prozessen entsprechen, die untersucht werden sollen. Sie können die Liste filtern, indem Sie in der Abfrage Platzhalterzeichen verwenden. ■ Ein Sternchen (*) entspricht keinem oder mehreren Zeichen. ■ Ein Fragezeichen (?) entspricht genau einem Zeichen. ■ Ein Ausrufezeichen (!) am Anfang einer Abfrage schließt alle Ergebnisse dieser Abfrage aus. Beispielsweise werden mit der folgenden Abfrage alle Prozesse ausgewählt, die mit **`ws`** beginnen, gleichzeitig werden auf **`sys`** endende Prozesse ausgeschlossen: **`'!*sys,ws*'`**

HINWEIS Einstellungen für Leistungsalarme gelten nur für View Connection Server- und View Agent-Systeme. Einstellungen für Leistungsalarme gelten nicht für View Client-Systeme.

Allgemeine Einstellungen

Tabelle 8-13 beschreibt die in der ADM-Vorlagendatei für die allgemeine View-Konfiguration enthaltenen allgemeinen Einstellungen.

Tabelle 8-13. Allgemeine View-Konfigurationsvorlage: Allgemeine Einstellungen

Einstellung	Eigenschaften
`Disk threshold for log and events in Megabytes`	Gibt den Speicherplatz an, der in Bezug auf die Ereignisprotokollierung mindestens auf der Festplatte verfügbar bleiben muss. Wenn kein Wert angegeben ist, lautet die Standardeinstellung 200. Nach Erreichen dieses Werts wird die Ereignisprotokollierung gestoppt.
`Enable extended logging`	Legt fest, ob trace- und debug-Ereignisse in die Protokolldateien geschrieben werden.

ADM-Vorlageneinstellungen für View-PCoIP-Sitzungsvariablen

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen (`pcoip.adm`) enthält Richtlinieneinstellungen in Bezug auf das PCoIP-Anzeigeprotokoll. Sie können die Einstellungen entweder mit den Standardwerten konfigurieren, die durch einen Administrator außer Kraft gesetzt werden können, oder die Einstellungen mit nicht überschreibbaren Werten konfigurieren.

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält zwei Unterkategorien:

Standardwerte, die durch einen Administrator außer Kraft gesetzt werden können	Gibt Standardwerte für PCoIP-Sitzungsvariablen an. Diese Einstellungen können durch einen Administrator außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults` geschrieben.
Einstellungen, die nicht durch einen Administrator außer Kraft gesetzt werden können	Enthält dieselben Einstellungen wie die erste Unterkategorie, diese Einstellungen können jedoch von einem Administrator nicht außer Kraft gesetzt werden. Für diese Einstellungen werden Werte in den Registrierungsschlüssel `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin` geschrieben.

Die Vorlage enthält ausschließlich Einstellungen für die Computerkonfiguration.

Nicht richtliniengesteuerte Registrierungsschlüssel

Wenn eine Einstellung auf einen lokalen Computer angewendet werden muss, die nicht in `HKLM\Software\Policies\Teradici` platziert werden kann, können die Einstellungen in Registrierungsschlüsseln unter `HKLM\Software\Teradici` eingefügt werden. In `HKLM\Software\Teradici` können dieselben Registrierungsschlüssel platziert werden wie in `HKLM\Software\Policies\Teradici`. Wenn ein Registrierungsschlüssel in beiden Verzeichnissen angegeben wurde, hat die Einstellung in `HKLM\Software\Policies\Teradici` Vorrang vor der Einstellung für den lokalen Computer.

- Allgemeine View-PCoIP-Sitzungsvariablen auf Seite 189

  Die ADM-Vorlagendatei für die View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen, mit denen allgemeine Sitzungskriterien wie PCoIP-Bildqualität, USB-Geräte und Netzwerkports konfiguriert werden.

- View-PCoIP-Sitzungsbandbreitenvariablen auf Seite 195

  Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsbandbreitenmerkmalen.

- View-PCoIP-Sitzungsvariablen für die Tastatur auf Seite 198

  Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsmerkmalen, die sich auf die Verwendung der Tastatur auswirken.

- View PCoIP Build-to-Lossless-Funktion auf Seite 199

  Das PCoIP-Anzeigeprotokoll verwendet eine Codierungsmethode namens „Progressive Build“ (Progressiver Aufbau), die auf die Gewährleistung einer optimalen allgemeinen Benutzerumgebung selbst unter eingeschränkten Netzwerkbedingungen abzielt.

Allgemeine View-PCoIP-Sitzungsvariablen

Die ADM-Vorlagendatei für die View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen, mit denen allgemeine Sitzungskriterien wie PCoIP-Bildqualität, USB-Geräte und Netzwerkports konfiguriert werden.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen

Einstellung	Beschreibung
`Configure clipboard redirection (Zwischenablageumleitung konfigurieren)`	Legt fest, in welche Richtung die Zwischenablageumleitung zugelassen ist. Es stehen folgende Werte zur Auswahl: ■ **[Enabled client to server only (Aktiviert, nur Client zu Server)]** (D.h. Kopieren und Einfügen nur vom Clientsystem zum View-Desktop zulassen.) ■ **[Disabled in both directions (Deaktiviert, beide Richtungen)]** ■ **[Enabled in both directions (Aktiviert, beide Richtungen)]** ■ **[Enabled server to client only (Aktiviert, nur Server zu Client)]** (D.h. Kopieren und Einfügen nur vom View-Desktop zum Clientsystem zulassen.) Die Zwischenablageumleitung wird als virtueller Kanal implementiert. Wenn virtuelle Kanäle deaktiviert sind, funktioniert die Zwischenablageumleitung nicht. Diese Einstellung gilt nur für den Server. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, lautet der Standardwert **[Enabled client to server only (Aktiviert, nur Client zu Server)]** .
`Configure PCoIP client image cache size policy (Richtlinie für PCoIP-Client-Bildcachegröße konfigurieren)`	Reguliert die Größe des PCoIP-Client-Bildcaches. Der Client verwendet die Bild-Zwischenspeicherung, um Teile der vorab übertragenen Anzeige zu speichern. Durch die Bild-Zwischenspeicherung wird die Menge der erneut übermittelten Daten minimiert. Diese Einstellung gilt nur für Windows- und Linux-Clients, wenn View Client, View Agent und View Connection Server auf View 5.0 oder einer neueren Version basieren. Ist diese Einstellung nicht konfiguriert oder deaktiviert, verwendet PCoIP eine Standard-Clientbildcachegröße von 250 MB. Bei Aktivierung dieser Einstellung können Sie die Client-Bildcachegröße von mindestens 50 MB auf 300 MB konfigurieren. Der Standardwert ist 250MB.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure PCoIP image quality levels (Stufen der PCoIP-Bildqualität konfigurieren)`	Steuert die PCoIP-Bilddarstellung während einer Netzwerküberlastung. Das Zusammenspiel der Werte **[Minimum Image Quality (Mindestqualität für Bilder)]**, **[Maximum Initial Image Quality (Maximale anfängliche Bildqualität)]** und **[Maximum Frame Rate (Maximale Frame-Rate)]** ermöglicht eine genaue Steuerung in Umgebungen mit begrenzter Netzwerkbandbreite. Verwenden Sie den Wert **[Minimum Image Quality (Mindestqualität für Bilder)]** zur Abstimmung von Bildqualität und Frame-Rate, wenn die Bandbreite begrenzt ist. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 50. Ein niedrigerer Wert ermöglicht höhere Frame-Rates, kann jedoch zu einer Beeinträchtigung der Anzeigequalität führen. Ein höherer Wert bietet eine höhere Bildqualität, unter Umständen jedoch niedrigere Frame-Rates, wenn die Netzwerkbandbreite begrenzt ist. Wenn die Netzwerkbandbreite keiner Einschränkung unterliegt, stellt PCoIP unabhängig von diesem Wert eine maximale Qualität sicher. Verwenden Sie die Einstellung **[Maximum Initial Image Quality (Maximale anfängliche Bildqualität)]**, um Spitzen bei der Belegung von Netzwerkbandbreite durch PCoIP zu vermeiden. Beschränken Sie hierzu die anfängliche Qualität der geänderten Bereiche für die Bildanzeige. Sie können einen Wert zwischen 30 und 100 angeben. Der Standardwert beträgt 90. Ein niedrigerer Wert verringert die Bildqualität bei Inhaltsänderungen und verhindert Spitzen bei der Bandbreitenbelegung. Ein höherer Wert verbessert die Bildqualität bei Inhaltsänderungen und erhöht die Bandbreitenanforderungen. Die nicht geänderten Bildbereiche erreichen unabhängig von diesem Wert stufenweise eine verlustfreie (perfekte) Qualität. Zur optimalen Nutzung der verfügbaren Bandbreite empfiehlt sich ein Wert von 90 oder niedriger. Der Wert **[Minimum Image Quality (Mindestqualität für Bilder)]** darf den Wert **[Maximum Initial Image Quality (Maximale anfängliche Bildqualität)]** nicht überschreiten. Verwenden Sie den Wert **[Maximum Frame Rate (Maximale Frame-Rate)]** zur Verwaltung der pro Benutzer durchschnittlich genutzten Bandbreite. Begrenzen Sie dazu die Anzahl der Bildschirmaktualisierungen pro Sekunde. Geben Sie einen Wert zwischen 1 und 120 Frames pro Sekunde an. Der Standardwert beträgt 30. Ein höherer Wert kann mehr Bandbreite belegen, jedoch weniger Jitter verursachen und so weichere Bildübergänge ermöglichen, z.B. bei einem Video. Bei einem geringeren Wert wird weniger Bandbreite belegt, allerdings mehr Jitter verursacht. Diese Werte für die Bildqualität gelten nur für den Softhost und haben auf einen Softclient keine Auswirkung. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, werden die Standardwerte verwendet.
`Configure PCoIP session encryption algorithms (Verschlüsselungsalgorithmen für PCoIP-Sitzung konfigurieren)`	Steuert die Verschlüsselungsalgorithmen, die vom PCoIP-Endpunkt während der Sitzungsaushandlung angeboten werden. Durch Aktivierung eines Kontrollkästchens wird der entsprechende Verschlüsselungsalgorithmus deaktiviert. Sie müssen mindestens einen Algorithmus aktivieren. Standardmäßig sind die Algorithmen Salsa20-256round12 und AES-128-GCM zur Aushandlung durch diesen Endpunkt verfügbar. Diese Einstellung gilt sowohl für den Server als auch für den Client. Die Endpunkte handeln den tatsächlich verwendeten Algorithmus für die Sitzungsverschlüsselung aus. Wenn der FIPS140-2-validierte Modus aktiviert ist, wird der Wert **[Disable AES-128-GCM encryption (AES-128-GCM-Verschlüsselung deaktivieren)]** immer außer Kraft gesetzt, sodass die AES-128-GCM-Verschlüsselung aktiviert wird. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, stehen die Algorithmen Salsa20-256round12 und AES-128-GCM zur Aushandlung durch diesen Endpunkt zur Verfügung.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure PCoIP USB allowed and unallowed device rules (In PCoIP-Sitzungen zugelassene und nicht zugelassene USB-Geräteregeln konfigurieren)`	Legt fest, welche USB-Geräte für PCoIP-Sitzungen autorisiert oder nicht autorisiert sind, die einen Zero-Client verwenden, der Teradici-Firmware ausführt. In PCoIP-Sitzungen verwendete USB-Geräte müssen in der USB-Autorisierungstabelle aufgeführt sein. USB-Geräte, die in der USB-Ausschlussliste erscheinen, können in PCoIP-Sitzungen nicht verwendet werden. Sie können maximal 10 USB-Autorisierungsregeln und höchstens 10 USB-Ausschlussregeln definieren. Trennen Sie mehrere Regeln durch einen senkrechten Strich (|) voneinander. Jede Regel kann eine Kombination aus einer Anbieter-ID und einer Produkt-ID sein, oder die Regel beschreibt eine Klasse von USB-Geräten. Eine Klassenregel kann eine gesamte Geräteklasse, eine einzelne Unterklasse oder ein Protokoll innerhalb einer Unterklasse zulassen oder ausschließen. Das Format einer kombinierten Regel aus Anbieter- und Produkt-ID lautet **`1xxxxyyyy`**, wobei **`xxxx`** die Anbieter-ID im Hexadezimalformat und **`yyyy`** die Produkt-ID im Hexadezimalformat darstellt. Die Regel zum Zulassen oder Sperren eines Geräts mit der Anbieter-ID **`0x1a2b`** und Produkt-ID **`0x3c4d`** würde beispielsweise **`11a2b3c4d`** lauten. Für Klassenregeln stehen folgende Formate zur Auswahl: **Alle USB-Geräte zulassen** Format: **`23XXXXXX`** Beispiel: **`23XXXXXX`** **USB-Geräte mit einer bestimmten Klassen-ID zulassen** Format: **`22`*`Klasse`*`XXXX`** Beispiel: **`22aaXXXX`** **Eine bestimmte Unterklasse zulassen** Format: **`21`*`Klasse-Unterklasse`*`XX`** Beispiel: **`21aabbXX`** **Ein bestimmtes Protokoll zulassen** Format: **`20`*`Klasse-Unterklasse-Protokoll`*** Beispiel: **`20aabbcc`** Die Zeichenfolge zur Autorisierung von USB-Eingabegeräten (Maus und Tastatur, Klassen-ID 0x03) und Webcams (Klassen-ID 0x0e) lautet beispielsweise **`2203XXXX|220eXXXX`**. Die Zeichenfolge zum Ausschließen von USB-Massenspeichergeräten (Klassen-ID 0x08) lautet **`2208XXXX`**. Eine leere Zeichenfolge für die USB-Autorisierung bedeutet, dass keine USB-Geräte zugelassen sind. Eine leere Zeichenfolge für den USB-Ausschluss bedeutet, dass für USB-Geräte keine Einschränkungen gelten. Diese Einstellung gilt ausschließlich für den Server und nur dann, wenn sich der Server in einer Sitzung mit einem Zero-Client befindet, der Teradici-Firmware ausführt. Die Geräteverwendung wird zwischen den Endpunkten ausgehandelt. Standardmäßig sind sämtliche Geräte zugelassen, und es sind keine Geräte ausgeschlossen.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure PCoIP virtual channels (Virtuelle PCoIP-Kanäle konfigurieren)`	Gibt die virtuellen Kanäle an, die bei PCoIP-Sitzungen verwendet bzw. nicht verwendet werden können. Diese Einstellung legt auch fest, ob die Zwischenablageverarbeitung auf dem PCoIP-Host deaktiviert wird. Virtuelle Kanäle, die in PCoIP-Sitzungen verwendet werden, müssen in der Tabelle der autorisierten virtuellen Kanäle aufgeführt sein. Virtuelle Kanäle, die in der Ausschlussliste für virtuelle Kanäle erscheinen, können in PCoIP-Sitzungen nicht verwendet werden. Sie können maximal 15 virtuelle Kanäle zur Verwendung in PCoIP-Sitzungen angeben. Trennen Sie mehrere Kanäle durch einen senkrechten Strich (|) voneinander. Die Zeichenfolge zum Zulassen der virtuellen Kanäle „mksvchan“ und „vdp_rdpvcbridge“ lautet z.B. **`mksvchan|vdp_vdpvcbridge`**. Wenn ein Kanalname einen senkrechten Strich oder einen umgekehrten Schrägstrich (\\) enthält, fügen Sie vor dem Kanalnamen einen umgekehrten Schrägstrich ein. Der Kanalname „awk|ward\channel“ wird beispielsweise folgendermaßen eingegeben: **`awk\\|ward\\channel`**. Ist die Tabelle der autorisierten virtuellen Kanäle leer, ist die Verwendung von virtuellen Kanälen nicht zulässig. Ist die Ausschlusstabelle für virtuelle Kanäle leer, sind alle virtuellen Kanäle zugelassen. Die Einstellung der virtuellen Kanäle gilt sowohl für den Server als auch für den Client. Zum Verwenden virtueller Kanäle müssen diese sowohl auf dem Server als auch auf dem Client aktiviert werden. Bei Festlegung der virtuellen Kanäle wird ein separates Kontrollkästchen angezeigt, mit dem Sie die Remote-Zwischenablageverarbeitung auf dem PCoIP-Host deaktivieren können. Dieser Wert gilt nur für den Server. Standardmäßig sind alle virtuellen Kanäle aktiviert, einschließlich der Zwischenablageverarbeitung.
`Configure the Client PCoIP UDP port (UDP-Port für PCoIP-Client konfigurieren)`	Gibt den UDP-Port an, der von Software-PCoIP-Clients verwendet wird. Der Wert des UDP-Ports gibt den zu verwendenden Basisport vor. Der Wert für den UDP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 50002 lautet und der Portbereich auf 64 festgelegt ist, umfasst der Bereich die Ports 50002 bis 50066. Diese Einstellung gilt nur für den Client. Standardmäßig lautet der Basisport 50002 und der Portbereich ist auf 64 festgelegt.
`Configure the TCP port to which the PCoIP host binds and listens (TCP-Port für PCoIP-Hostbindung und -Überwachung konfigurieren)`	Gibt den TCP-Serverport für Software-PCoIP-Hosts an. Der Wert des TCP-Ports gibt den TCP-Basisport für die Serverbindung an. Der TCP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 0 und 10 liegen. Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182. Diese Einstellung gilt nur für den Server. Für View 4.5 und höhere Versionen lautet der TCP-Port standardmäßig 4172, für View 4.0.*x* und frühere Versionen wird standardmäßig Port 50002 verwendet. Der Portbereich lautet standardmäßig 1.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
Configure the UDP port to which the PCoIP host binds and listens (UDP-Port für PCoIP-Hostbindung und -Überwachung konfigurieren)	Gibt den UDP-Serverport für Software-PCoIP-Hosts an. Der Wert des UDP-Ports gibt den UDP-Basisport für die Serverbindung an. Der Wert für den UDP-Portbereich legt fest, wie viele zusätzliche Ports ausprobiert werden, falls der Basisport nicht verfügbar ist. Der Portbereich muss zwischen 0 und 10 liegen. Der Bereich erstreckt sich vom Basisport bis zur Summe aus Basisport und Portbereich. Wenn der Basisport beispielsweise 4172 lautet und der Portbereich auf 10 festgelegt ist, umfasst der Bereich die Ports 4172 bis 4182. Diese Einstellung gilt nur für den Server. Für View 4.5 und höhere Versionen lautet der TCP-Port standardmäßig 4172, für View 4.0.*x* und frühere Versionen wird standardmäßig Port 50002 verwendet. Der Portbereich lautet standardmäßig 10.
Enable access to a PCoIP session from a vSphere console (Zugriff auf PCoIP-Sitzung von einer vSphere-Konsole aus zulassen)	Legt fest, ob in einer vSphere Client-Konsole die Anzeige einer aktiven PCoIP-Sitzung und das Senden von Eingaben an den Desktop gestattet werden soll. Standardmäßig zeigt der Bildschirm der vSphere Client-Konsole nichts an, wenn ein Client über PCoIP verbunden ist, und die Konsole kann keine Eingaben senden. Diese Standardeinstellung verhindert, dass ein anderer Benutzer den Desktop des Benutzers anzeigen kann oder mit böswilligen Absichten lokal am Host Eingaben vornimmt, während eine PCoIP-Remote-Sitzung aktiv ist. Diese Einstellung gilt nur für den Server. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist ein Konsolenzugriff nicht zulässig. Wenn diese Einstellung aktiviert ist, zeigt die Konsole die PCoIP-Sitzung an und eine Konsoleneingabe ist zulässig. Wenn diese Einstellung aktiviert ist, kann die Konsole nur dann eine PCoIP-Sitzung anzeigen, die mit einem Windows 7-System ausgeführt wird, wenn die virtuelle Maschine für Windows 7 mit Hardware v8 arbeitet. Hardware v8 ist nur für ESX 5.0 und neuere Versionen verfügbar. Im Gegensatz hierzu sind Konsoleneingaben in ein Windows 7-System für alle Hardwareversionen der virtuellen Maschinen zulässig. Auf Windows XP- oder Windows Vista-Systemen kann die Konsole eine PCoIP-Sitzung anzeigen, wenn die virtuelle Maschine über egal welche Hardwareversion verfügt.
Enable the FIPS 140-2 approved mode of operation (FIPS 140-2-validierten Betriebsmodus aktivieren)	Legt fest, ob zum Herstellen einer Remote-PCoIP-Verbindung ausschließlich FIPS 140-2-validierte kryptografische Algorithmen und Protokolle verwendet werden dürfen. Die Aktivierung dieser Einstellung setzt die Deaktivierung der AES128-GCM-Verschlüsselung außer Kraft. Diese Einstellung gilt sowohl für den Server als auch für den Client. Sie können entweder einen oder beide Endpunkte zum Betrieb im FIPS-Modus konfigurieren. Das Konfigurieren eines einzigen Endpunkts im FIPS-Modus begrenzt die bei der Sitzungsaushandlung verfügbaren Verschlüsselungsalgorithmen. Der FIPS-Modus ist für View 4.5 und höhere Versionen verfügbar. Für View 4.0.*x* und frühere Versionen steht der FIPS-Modus nicht zur Verfügung, daher hat eine Konfiguration dieser Einstellung keine Auswirkung. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird der FIPS-Modus nicht verwendet.
Enable/disable audio in the PCoIP session (Audio für PCoIP-Sitzung aktivieren/deaktivieren)	Legt fest, ob die Audiofunktion während PCoIP-Sitzungen aktiviert ist. Die Audiofunktion muss für beide Endpunkte aktiviert sein. Ist diese Einstellung aktiviert, ist die Verwendung von PCoIP-Audio zulässig. Wurde diese Einstellung deaktiviert, kann die PCoIP-Audiofunktion nicht verwendet werden. Wurde diese Einstellung nicht konfiguriert, ist die Audiofunktion standardmäßig aktiviert.

Tabelle 8-14. Allgemeine View-PCoIP-Sitzungsvariablen (Fortsetzung)

Einstellung	Beschreibung
`Enable/disable microphone noise and DC offset filter in PCoIP session (Mikrofongeräusche und Gleichstrom-Offset-Filter in PCoIP-Sitzung aktivieren/deaktivieren)`	Legt fest, ob Mikrofongeräusche und der Gleichstrom-Offset-Filter für die Mikrofoneingabe während der PCoIP-Sitzung aktiviert werden sollen. Diese Einstellung gilt nur für den Server und den Teradici-Audiotreiber. Wenn diese Einstellung nicht konfiguriert ist, verwendet der Teradici-Audiotreiber standardmäßig die Mikrofongeräusche und den Gleichstrom-Offset-Filter.
`Turn on PCoIP user default input language synchronization (Synchronisierung der Standardeingabesprache für PCoIP-Benutzer aktivieren)`	Legt fest, ob die Standardeingabesprache des Benutzers in der PCoIP-Sitzung mit der standardmäßigen Eingabesprache des PCoIP-Clientendpunktes synchronisiert wird. Wenn diese Einstellung aktiviert ist, ist eine Synchronisierung zugelassen. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, ist eine Synchronisierung nicht erlaubt. Diese Einstellung gilt nur für den Server.

View-PCoIP-Sitzungsbandbreitenvariablen

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsbandbreitenmerkmalen.

Tabelle 8-15. View-PCoIP-Sitzungsbandbreitenvariablen

Einstellung	Beschreibung
`Configure the maximum PCoIP session bandwidth (Maximale PCoIP-Sitzungsbandbreite konfigurieren)`	Legt die maximale Bandbreite für eine PCoIP-Sitzung in Kilobits pro Sekunde fest. Die Bandbreite umfasst den gesamten Sitzungsdatenverkehr von Bilddarstellung, Audio, virtuellen Kanälen, USB und PCoIP-Steuerung. Legen Sie diesen Wert auf die Gesamtkapazität der Verbindung fest, über die Ihr Endpunkt verbunden ist. Beispielsweise legen Sie diesen Wert für einen Client, der eine 4 MBit/s-Internetverbindung verwendet, auf 4 MBit oder einen 10% niedrigeren Wert fest. Durch eine Festlegung dieses Werts verhindern Sie, dass der Server eine die Verbindungskapazität übersteigende Übertragungsrate wählt – was zu einem übermäßigen Paketverlust und einem schlechteren Benutzererlebnis führen würde. Dieser Wert ist symmetrisch. Client und Server werden gezwungen, den niedrigeren der beiden Werte zu verwenden, die auf Client- und Serverseite festgelegt sind. Beispielsweise wird der Server bei Festlegung einer maximalen Bandbreite von 4 MBit/s gezwungen, eine niedrigere Übertragungsrate zu verwenden – auch wenn die Einstellung auf dem Client konfiguriert ist. Wenn diese Einstellung deaktiviert wurde oder auf einem Endpunkt nicht konfiguriert ist, legt der Endpunkt keine Bandbreiteneinschränkungen fest. Wenn diese Einstellung konfiguriert ist, wird sie als maximale Bandbreiteneinschränkung des Endpunkts in KBit/s verwendet. Der Standardwert für die nicht konfigurierte Einstellung liegt bei 90000 KBit/s. Diese Einstellung gilt sowohl für den Server als auch für den Client. Haben die beiden Endpunkte unterschiedliche Einstellungen, wird der niedrigere Wert verwendet.
`Configure the PCoIP session bandwidth floor (PCoIP-Mindestsitzungsbandbreite konfigurieren)`	Legt die Mindestbandbreite in Kilobits pro Sekunde fest, die von der PCoIP-Sitzung reserviert wird. Mit dieser Einstellung wird die minimale erwartete Bandbreitenübertragungsrate für den Endpunkt konfiguriert. Wenn Sie diese Einstellung zum Reservieren der Bandbreite für einen Endpunkt verwenden, muss der Benutzer nicht warten, bis Bandbreite verfügbar ist, was die Reaktionszeit während der Sitzung verbessert. Achten Sie jedoch darauf, dass Sie allen Endpunkten gemeinsam nicht mehr Bandbreite zuweisen, als insgesamt zur Verfügung steht. Die Summe der Mindestbandbreitenwerte für alle Verbindungen in Ihrer Konfiguration darf die Netzwerkkapazität nicht überschreiten. Der Standardwert lautet 0, d.h. es wird keine Mindestbandbreite reserviert. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird keine Mindestbandbreite reserviert. Diese Einstellung gilt sowohl für den Server als auch für den Client, wirkt sich allerdings nur auf den Endpunkt aus, für den sie konfiguriert wurde.

Tabelle 8-15. View-PCoIP-Sitzungsbandbreitenvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the PCoIP session MTU (Maximale Übertragungseinheit für PCoIP-Sitzung konfigurieren)`	Legt die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für UDP-Pakete bei einer PCoIP-Sitzung fest. Die MTU-Größe umfasst den IP- und UDP-Paketvorspann. TCP verwendet den standardmäßigen MTU-Ermittlungsmechanismus zum Festlegen der maximalen Übertragungseinheit und wird von dieser Einstellung nicht beeinflusst. Die maximale MTU-Größe beträgt 1.500 Byte. Die minimale MTU-Größe beträgt 500 Byte. Der Standardwert lautet 1.300 Byte. Normalerweise muss die MTU-Größe nicht geändert werden. Ändern Sie diesen Wert, wenn Sie in einer nicht standardmäßig eingerichteten Netzwerkumgebung arbeiten, die zu einer PCoIP-Paketfragmentierung führt. Diese Einstellung gilt sowohl für den Server als auch für den Client. Unterscheiden sich die MTU-Größeneinstellungen der beiden Endpunkte, wird der niedrigere Wert verwendet. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, verwendet der Client bei der Aushandlung mit dem Server den Standardwert.

Tabelle 8-15. View-PCoIP-Sitzungsbandbreitenvariablen (Fortsetzung)

Einstellung	Beschreibung
`Configure the PCoIP session audio bandwidth limit (Audiobandbreitenlimit für PCoIP-Sitzung konfigurieren)`	Legt die maximale Bandbreite fest, die in einer PCoIP-Sitzung für Audiodaten (Soundwiedergabe) verwendet werden kann. Der Audioprozessor überwacht die für Audiodaten verwendete Bandbreite. Er wählt auch den Algorithmus zur Audiokomprimierung, der bei der aktuellen Bandbreitennutzung die bestmögliche Audioqualität liefert. Wenn ein Bandbreitenlimit festgelegt wurde, reduziert der Audioprozessor durch einen Wechsel des Komprimierungsalgorithmus so lange die Qualität, bis das Bandbreitenlimit erreicht ist. Wenn die minimale Audioqualität mit dem festgelegten Bandbreitenlimit nicht erreicht werden kann, wird die Audiofunktion deaktiviert. Stellen Sie diesen Wert höher als 1.600 KBit/s ein, um Audiodaten nicht zu komprimieren und eine hohe Stereo-Qualität zu erzielen. Ein Wert ab 450 KBit/s bietet Stereo-Qualität mit komprimierten Audiodaten. Ein Wert zwischen 50 KBit/s und 450 KBit/s liefert eine Audioqualität, die zwischen einem UKW-Radio und einem Telefongespräch liegt. Bei einem Wert unter 50 KBit/s ist unter Umständen keine Audiowiedergabe mehr möglich. Diese Einstellung gilt nur für den Server. Diese Einstellung wird erst wirksam, wenn Sie die Audiofunktion an beiden Endpunkten aktivieren. Zudem hat diese Einstellung keinerlei Auswirkungen auf USB-Audio. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird standardmäßig ein Bandbreitenlimit von 500 KBit/s konfiguriert, um den ausgewählten Algorithmus für die Audiokomprimierung zu begrenzen. Bei Konfiguration dieser Einstellung wird der Wert in KBit/s gemessen, mit einem standardmäßigen Audiobandbreitenlimit von 500 KBit/s. Diese Einstellung gilt für View 4.6 und höhere Versionen. Bei früheren View-Versionen hat diese Einstellung keine Auswirkung.
`Turn off Build-to-Lossless feature (Build-to-Lossless-Funktion abschalten)`	Legt fest, ob die Build-to-Lossless-Funktion des PCoIP-Protokolls deaktiviert werden soll, obwohl sie standardmäßig aktiviert ist. Wenn Sie diese Einstellung aktivieren, wird die Build-to-Lossless-Funktion deaktiviert. Bilder und andere Desktop-Inhalte werden nie zu einem verlustfreien Anzeigestadium aufgebaut. In Netzwerkumgebungen mit begrenzter Bandbreite kann die Deaktivierung der Build-to-Lossless-Funktion Einsparungen bei der Bandbreite ermöglichen. Das Deaktivieren dieser Funktion wird für Umgebungen, in denen ein Aufbau von Bildern und Desktop-Inhalten zu einem verlustfreien Anzeigestadium erforderlich ist, nicht empfohlen. Um diese Einstellung zu aktivieren, müssen Sie auf **[Enabled (Aktiviert)]** klicken und einen Haken in das folgende Kontrollkästchen setzen: **[I accept to turn off the Build-to-Lossless feature (Ich stimme der Abschaltung der Build-to-Lossless-Funktion zu)]** . Durch diese Bestätigung akzeptieren und verstehen Sie, dass Bilder und Desktop-Inhalte nie zu einem verlustfreien Anzeigestadium aufgebaut werden. Weitere Informationen über die PCoIP-Build-to-Lossless-Funktion finden Sie unter „View PCoIP Build-to-Lossless-Funktion“, auf Seite 199.

View-PCoIP-Sitzungsvariablen für die Tastatur

Die ADM-Vorlagendatei für View-PCoIP-Sitzungsvariablen enthält Gruppenrichtlinieneinstellungen zur Konfiguration von PCoIP-Sitzungsmerkmalen, die sich auf die Verwendung der Tastatur auswirken.

Tabelle 8-16. View-PCoIP-Sitzungsvariablen für die Tastatur

Einstellung	Beschreibung
Disable sending CAD when users press Ctrl+Alt+Del (Senden eines Sicherheitsaufrufs für Strg+Alt+Entf deaktivieren)	Wenn diese Richtlinie aktiviert ist, müssen Benutzer anstelle der Tastenkombination Strg+Alt+Entf die Tastenkombination Strg+Alt+Einfg drücken, um während einer PCoIP-Sitzung einen Sicherheitsaufruf (Secure Attention Sequence, SAS) an den Desktop zu senden. Sie können diese Einstellung aktivieren, um eine Verwirrung der Benutzer zu vermeiden, wenn diese zum Sperren des Clientendpunktes Strg+Alt +Entf drücken, und sowohl an den Host als auch an den Gast ein Sicherheitsaufruf gesendet wird. Diese Einstellung gilt nur für den Server und hat auf einen Client keine Auswirkung. Wenn diese Richtlinie nicht konfiguriert ist oder deaktiviert wurde, können Benutzer die Tastenkombination Strg+Alt+Entf oder Strg+Alt+Einfg drücken, um einen Sicherheitsaufruf an den Desktop zu senden.
Enable Right SHIFT behavior when a PCoIP client is connected (Rechte Umschalttaste aktivieren, wenn ein PCoIP-Client verbunden ist)	Legt fest, ob die rechte Umschalttaste durch die linke Umschalttaste ersetzt wird, wodurch die ordnungsgemäße Funktion der rechten Umschalttaste bei Verwendung von RDP über PCoIP sichergestellt wird. Diese Einstellung kann nützlich sein, wenn RDP innerhalb einer PCoIP-Sitzung verwendet wird. Diese Einstellung gilt nur für den Server und hat auf einen Client keine Auswirkung. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, findet keine Ersetzung statt. Auf Desktops mit View Agent 4.6 oder höher funktioniert die rechte Umschalttaste ordnungsgemäß, wenn in einer PCoIP-Sitzung RDP verwendet wird. Verwenden Sie diese Einstellung nur auf Desktops, auf denen View Agent 4.5 oder eine frühere Version ausgeführt wird. Für View Agent 4.6 wird diese Einstellung angewendet, sie ist aber nicht erforderlich. Für View Agent 5.0 und höher wird diese Einstellung auch dann nicht angewendet, wenn sie konfiguriert ist.

Tabelle 8-16. View-PCoIP-Sitzungsvariablen für die Tastatur (Fortsetzung)

Einstellung	Beschreibung
`Use alternate key for sending Secure Attention Sequence (Alternative Taste für Sicherheitsaufruf verwenden)`	Gibt eine alternative Taste (anstelle der Einfg-Taste) zum Senden eines Sicherheitsaufrufs (Secure Attention Sequence, SAS) an. Sie können mit dieser Einstellung die Tastenkombination Strg+Alt+Einfg in virtuellen Maschinen beibehalten, die während einer PCoIP-Sitzung aus einem View-Desktop gestartet werden. Beispielsweise kann ein Benutzer eine vSphere Client-Instanz aus einem PCoIP-Desktop starten und auf einer virtuellen Maschine in vCenter Server eine Konsole öffnen. Wenn die Tastenkombination Strg+Alt+Einfg im Gastbetriebssystem auf der virtuellen vCenter Server-Maschine verwendet wird, wird ein Strg+Alt+Entf-Sicherheitsaufruf an die virtuelle Maschine gesendet. Diese Einstellung ermöglicht, dass mit der Tastenkombination Strg+Alt+*Alternative Taste* ein Strg+Alt+Entf-Sicherheitsaufruf an den PCoIP-Desktop gesendet wird. Wenn diese Einstellung aktiviert ist, müssen Sie eine alternative Taste aus einem Dropdown-Menü auswählen. Es ist nicht möglich, die Einstellung zu aktivieren und keinen Wert anzugeben. Wenn diese Einstellung deaktiviert wurde oder nicht konfiguriert ist, wird die Tastenkombination Strg+Alt+Einfg zum Senden eines Sicherheitsaufrufs verwendet. Diese Einstellung gilt nur für den Server und hat auf einen Client keine Auswirkung.
`Use enhanced keyboard on Windows client if available (Erweiterte Tastatur auf Windows-Client verwenden, falls verfügbar)`	Legt fest, ob die Tastatur-Sequenzen auf das Gastbetriebssystem der PCoIP-Desktop-Sitzungen beschränkt werden soll. Wenn Sie Strg+Alt+Entf, Win+L oder eine andere Tastatur-Sequenz drücken, reagiert nur das Gastsystem (und nicht etwa sowohl Gast und Host) auf den Befehl. Durch Betätigen von Strg+Alt+Entf wird das Hostsystem beispielsweise nicht gesperrt. Diese Einstellung gilt nur für Windows-Hosts. Bevor die erweiterten Tastatureinstellungen greifen können, muss der VMware-Tastaturfiltertreiber, `vmkbd.sys`, installiert und konfiguriert werden. Der VMware-Tastaturfiltertreiber ist auf Computern, die über VMware Workstation, Player oder View Client with Local Mode verfügen, automatisch installiert und konfiguriert. Sie können diese Einstellung nur verwenden, wenn View Client von einem Mitglied der Administratorgruppe auf Windows XP oder unter erweiterten Zugriffsrechten durch **die Option „Als Administrator ausführen“** auf Windows Vista und neueren Versionen ausgeführt wird. Diese Einstellung ermöglicht es dem Windows-Hostsystem, die Tastatureingaben durch eine alternative Methode zu verarbeiten. Sie verarbeitet unformatierte Tastatureingaben so schnell wie möglich und umgeht dabei die Windows-Tastaturanschlag-Aufbereitungsmethode sowie jegliche schädliche Software, die sich nicht bereits auf einer weiter unten liegenden Ebene befindet. Verwenden Sie die erweiterte virtuelle Tastatur, wenn die virtuelle Maschine sonst von jemandem mit einer internationalen Tastatur oder einer Tastatur mit zusätzlichen Tasten verwendet werden könnte. Wenn diese Richtlinie nicht konfiguriert oder deaktiviert ist, wird die erweiterte Tastaturfunktion nicht verwendet.

View PCoIP Build-to-Lossless-Funktion

Das PCoIP-Anzeigeprotokoll verwendet eine Codierungsmethode namens „Progressive Build“ (Progressiver Aufbau), die auf die Gewährleistung einer optimalen allgemeinen Benutzerumgebung selbst unter eingeschränkten Netzwerkbedingungen abzielt.

„Progressive Build“ bietet ein hochgradig komprimiertes Erstbild, auch „verlustbehaftetes Bild“ genannt, welches dann stufenweise zu einem vollständig verlustfreien Anzeigestadium erweitert wird. Unter einem „verlustfreien Stadium“ versteht man, dass das Bild mit der beabsichtigten Originaltreue angezeigt wird.

In einem LAN zeigt PCoIP Text immer unter Verwendung der verlustfreien Komprimierung an. Sinkt die verfügbare Bandbreite pro Sitzung auf unter 1 MB, zeigt PCoIP zuerst ein verlustbehaftetes Textbild an und baut das Bild dann innerhalb kürzester Zeit zu einem verlustfreien Anzeigestadium auf. Durch diese Vorgehensweise kann der Desktop weiterhin reagieren und auch bei wechselnden Netzwerkbedingungen das bestmögliche Bild anzeigen, was zu einer optimalen Benutzererfahrung führt.

Die Build-to-Lossless-Funktion verfügt über folgende Leistungsmerkmale:

- Dynamische Anpassung der Bildqualität
- Verringerung der Bildqualität in überlasteten Netzwerken
- Aufrechterhaltung der Reaktionsfähigkeit durch Minimierung der Wartezeiten bei der Bildschirmaktualisierung
- Wiederaufnahme der maximalen Bildqualität nach Beheben der Netzwerküberlastung

Das PCoIP-Protokoll ist effizient genug, um die Build-to-Lossless-Funktion unter allen Bedingungen zur Verfügung zu stellen, weshalb diese Funktion standardmäßig aktiviert bleiben kann.

Sie können die Funktion „Build-to-Lossless“ deaktivieren, indem Sie die Gruppenrichtlinieneinstellung `Turn off Build-to-Lossless feature (Build-to-Lossless-Funktion abschalten)` einrichten. Siehe „View-PCoIP-Sitzungsbandbreitenvariablen“, auf Seite 195.

Einrichten des standortbasierten Drucks

Die standortbasierte Druckfunktion ordnet Drucker, die sich physisch in der Nähe von Clientsystemen befinden, View-Desktops zu. Auf diese Weise können Benutzer von ihren View-Desktops über ihre lokalen Drucker oder Netzwerkdrucker drucken.

Die standortbasierte Druckfunktion ist sowohl für Windows- als auch Windows-fremde Clientsysteme verfügbar. Der standortbasierte Druck ermöglicht es IT-Organisationen, View-Desktops dem Drucker zuzuordnen, der sich am nahesten am Endpunkt-Clientgerät befindet. Wenn ein Arzt im Krankenhaus sich beispielsweise von Raum zu Raum bewegt, wird der Druckauftrag bei jedem Ausdrucken eines Dokuments an den nächstgelegenen Drucker gesendet. Bei Verwendung dieser Funktion müssen die korrekten Druckertreiber nicht auf dem View-Desktop installiert sein.

Sie richten den standortbasierten Druck ein, indem Sie die Active Directory-Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)` konfigurieren, die sich im Gruppenrichtlinienobjekt-Editor von Microsoft im Ordner **[Software Settings (Softwareeinstellungen)]** unter **[Computer Configuration (Computerkonfiguration)]** befindet.

Hinweis `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)` ist eine computerspezifische Richtlinie. Computerspezifische Richtlinien gelten für alle View-Desktops, unabhängig davon, wer sich mit dem Desktop verbindet.

`AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)` ist als eine Tabelle für die Namensübersetzung implementiert. Sie verwenden jede Zeile in der Tabelle, um einen bestimmten Drucker zu identifizieren und einen Satz an Übersetzungsregeln für diesen Drucker zu definieren. Die Übersetzungsregeln legen fest, ob der Drucker zum View-Desktop für ein bestimmtes Clientsystem zugeordnet wird.

Wenn sich ein Benutzer mit einem View-Desktop verbindet, vergleicht View das Clientsystem mit den Übersetzungsregeln, die mit jedem Drucker in der Tabelle verknüpft sind. Wenn das Clientsystem allen Übersetzungsregeln für einen Drucker entspricht, oder wenn mit einem Drucker keine Übersetzungsregeln verknüpft sind, ordnet View den Drucker während der Benutzersitzung dem View-Desktop zu.

Sie können Übersetzungsregeln basierend auf der IP-Adresse, dem Namen und der MAC-Adresse des Clientsystems sowie basierend auf dem Benutzernamen und der Benutzergruppe definieren. Sie können für einen bestimmten Drucker eine Übersetzungsregel oder eine Kombination aus mehreren Übersetzungsregeln festlegen.

Die Informationen für die Zuordnung des Druckers zum View-Desktop werden in einem Eintrag im Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect` auf dem View-Desktop gespeichert.

1 Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck auf Seite 201

   Um die Gruppenrichtlinieneinstellung für den standortbasierten Druck konfigurieren zu können, muss die DLL-Datei `TPVMGPoACmap.dll` registriert werden.

2 Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck auf Seite 201

   Um den standortbasierten Druck einzurichten, konfigurieren Sie die Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)`. Die Gruppenrichtlinieneinstellung ist eine Tabelle mit Namensübersetzungen, die Drucker zu View-Desktops zuordnet.

Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck

Um die Gruppenrichtlinieneinstellung für den standortbasierten Druck konfigurieren zu können, muss die DLL-Datei `TPVMGPoACmap.dll` registriert werden.

View stellt im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` auf dem View Connection Server-Host 32-Bit- und 64-Bit-Versionen der Datei `TPVMGPoACmap.dll` bereit.

Vorgehensweise

1 Kopieren Sie die geeignete Version der DLL-Datei `TPVMGPoACmap.dll` auf Ihren Active Directory-Server oder den Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.

2 Verwenden Sie das Dienstprogramm `regsvr32`, um die Datei `TPVMGPoACmap.dll` zu registrieren.

   Beispiel: `regsvr32 "C:\TPVMGPoACmap.dll"`

Weiter

Konfigurieren Sie die Gruppenrichtlinieneinstellung für den standortbasierten Druck.

Konfigurieren der Gruppenrichtlinie für den standortbasierten Druck

Um den standortbasierten Druck einzurichten, konfigurieren Sie die Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)`. Die Gruppenrichtlinieneinstellung ist eine Tabelle mit Namensübersetzungen, die Drucker zu View-Desktops zuordnet.

Voraussetzungen

- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server oder dem Domänencomputer zur Verfügung stehen, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden.
- Registrieren Sie die DLL-Datei `TPVMGPoACmap.dll` auf Ihrem Active Directory-Server oder dem Domänencomputer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden. Siehe „Registrieren der Gruppenrichtlinien-DLL für den standortbasierten Druck“, auf Seite 201.
- Machen Sie sich mit der Syntax der Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)` vertraut. Siehe „Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck“, auf Seite 202.

- Erstellen Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für die Gruppenrichtlinieneinstellung für den standortbasierten Druck und verknüpfen Sie es mit der Organisationseinheit (Organizational Unit, OU), die Ihre View-Desktops enthält. Siehe „Erstellen von GPOs für View-Gruppenrichtlinien“, auf Seite 207 finden Sie ein Beispiel für die Erstellung von GPOs für View-Gruppenrichtlinien.
- Da Druckaufträge direkt vom View-Desktop zum Drucker gesendet werden, müssen Sie sicherstellen, dass die erforderlichen Druckertreiber auf Ihren Desktops installiert sind.

Vorgehensweise

1 Wählen Sie auf Ihrem Active Directory-Server (oder dem Computer, den Sie zum Konfigurieren von Gruppenrichtlinien verwenden) **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Desktops enthält, und wählen Sie **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellung für den standortbasierten Druck erstellt haben, und wählen Sie **[Edit (Bearbeiten)]** .

Das Fenster Group Policy Object Editor (Gruppenrichtlinienobjekt-Editor) wird angezeigt.

5 Erweitern Sie die Ansicht **[Computer Configuration (Computerkonfiguration)]** , öffnen Sie den Ordner **[Software Settings (Softwareeinstellungen)]** und wählen Sie **[AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)]** aus.

6 Doppelklicken Sie im Fensterbereich „Policy (Richtlinie)“ auf **[Configure AutoConnect Map Additional Printers (Automatische Zuordnung zusätzlicher Drucker konfigurieren)]** .

Das Fenster AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View) wird angezeigt.

7 Wählen Sie die Option **[Enabled (Aktiviert)]** , um die Gruppenrichtlinieneinstellung zu aktivieren.

Im Gruppenrichtlinienfenster werden die Überschriften und Schaltflächen der Übersetzungstabelle angezeigt.

WICHTIG Durch Klicken auf **[Disabled (Deaktiviert)]** werden alle Tabelleneinträge gelöscht. Als Vorsichtsmaßnahme sollten Sie Ihre Konfiguration speichern, um sie später importieren zu können.

---

8 Fügen Sie alle Drucker hinzu, die Sie View-Desktops zuordnen möchten, und definieren Sie die zugehörigen Übersetzungsregeln.

9 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Syntax einer Gruppenrichtlinieneinstellung für den standortbasierten Druck

Sie verwenden die Gruppenrichtlinieneinstellung `AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)`, um Drucker zu View-Desktops zuzuordnen.

`AutoConnect Map Additional Printers for VMware View (Automatische Zuordnung zusätzlicher Drucker für VMware View)` ist eine Tabelle für die Namensübersetzung, die Drucker identifiziert und verknüpfte Übersetzungsregeln definiert. Tabelle 8-17 beschreibt die Syntax der Übersetzungstabelle.

Tabelle 8-17. Spalten und Werte in der Übersetzungstabelle

Spalte	Beschreibung
IP-Bereich	Eine Übersetzungsregel, die einen Bereich mit IP-Adressen für Clientsysteme angibt. Verwenden Sie die folgende Notierung, um IP-Adressen in einem bestimmten Bereich anzugeben: ***IP-Adresse-IP-Adresse*** Beispiel: **10.112.116.0-10.112.119.255** Verwenden Sie die folgende Notierung, um alle IP-Adressen in einem bestimmten Subnetz anzugeben: *IP-Adresse/Subnetzmasken-Bits* Beispiel: **10.112.4.0/22** Diese Notierung gibt die verwendbaren IPv4-Adressen von 10.112.4.1 bis 10.112.7.254 an. Geben Sie für eine beliebige IP-Adresse ein Sternchen (*) ein.
Clientname	Eine Übersetzungsregel, die einen Computernamen angibt. Beispiel: **Marias Computer** Geben Sie für einen beliebigen Computernamen ein Sternchen (*) ein.
Mac-Adresse	Eine Übersetzungsregel, die eine MAC-Adresse angibt. Im GPO-Editor muss dasselbe Format wie im Clientsystem verwendet werden. Beispiel: ■ Windows-Clients verwenden Bindestriche: **01-23-45-67-89-ab** ■ Linux-Clients verwenden Doppelpunkte: **01:23:45:67:89:ab** Geben Sie für eine beliebige MAC-Adresse ein Sternchen (*) ein.
Benutzer/Gruppe	Eine Übersetzungsregel, die einen Benutzer oder eine Benutzergruppe angibt. Beispiel: **jdoe** Geben Sie für einen beliebigen Benutzernamen bzw. eine beliebige Benutzergruppe ein Sternchen (*) ein.
Druckername	Der Name des Druckers bei der Zuweisung zum View-Desktop. Beispiel: **DRUCKER-2-CLR** Der zugewiesene Name muss nicht dem Druckernamen auf dem Clientsystem entsprechen.
Druckertreiber	Der Name des Treibers, den der Drucker verwendet. Beispiel: **HP Color LaserJet 4700 PS** **Wichtig** Da Druckaufträge direkt vom Desktop zum Drucker gesendet werden, muss der Druckertreiber auf dem Desktop installiert sein.
IP Port/ThinPrint Port (IP-Port/ThinPrint-Port)	Für Netzwerkdrucker wird der IP-Adresse des Druckers das Präfix **IP_** vorangestellt. Beispiel: **IP_10.114.24.1**
Standard	Gibt an, ob es sich bei dem Drucker um den Standarddrucker handelt.

Sie verwenden die Schaltflächen, die oberhalb der Spaltenüberschriften angezeigt werden, um Tabelleneinträge hinzuzufügen, zu löschen, Zeilen zu verschieben und zu importieren. Jede Schaltfläche verfügt über eine äquivalente Tastaturkombination. Bewegen Sie die Maus über jede Schaltfläche, um eine Beschreibung der Schaltfläche und die zugehörige Tastaturkombination anzuzeigen. Um beispielsweise eine Zeile am Ende der Tabelle einzufügen, klicken Sie auf die erste Tabellenschaltfläche und drücken Alt+A. Klicken Sie auf die letzten zwei Schaltflächen, um Tabelleneinträge zu importieren und zu speichern.

Tabelle 8-18 zeigt ein Beispiel für zwei Zeilen einer Übersetzungstabelle.

Tabelle 8-18. Gruppenrichtlinieneinstellung für den standortbasierten Druck – Beispiel

IP-Bereich	Clientname	Mac-Adresse	Benutzer/Gruppe	Druckername	Druckertreiber	IP Port/ThinPrint Port (IP-Port/ThinPrint-Port)	Standard
*	*	*	*	DRUCKER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	DRUCKER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

Der in der ersten Zeile angegebene Netzwerkdrucker wird einem View-Desktop für ein beliebiges Clientsystem zugeordnet, da in allen Spalten für die Übersetzungsregeln Sternchen angezeigt werden. Der in der zweiten Zeile angegebene Netzwerkdrucker wird nur dann einem View-Desktop zugeordnet, wenn sich die IP-Adresse des Clientsystems im Bereich 10.112.116.140 bis 10.112.116.145 befindet.

Verwenden von Terminaldienste-Gruppenrichtlinien

Sie können standardmäßige Gruppenrichtlinien für Microsoft Windows-Terminaldienste zur zentralen Steuerung der Konfiguration von View-Desktops einsetzen.

Bei Windows Vista und neueren Betriebssystemen werden die Terminaldienste als Remote-Desktop-Dienste bezeichnet.

Hinweis Die Terminaldienste müssen auf der virtuellen Maschine gestartet werden, die Sie zur Erstellung von Pools und auf View-Desktops verwenden. Die Terminaldienste sind erforderlich für die Installation von View Agent, SSO und andere View-Sitzungsverwaltungsvorgänge.

Um die Terminaldienste-Gruppenrichtlinieneinstellung im Gruppenrichtlinienobjekt-Editor einzusehen, müssen Sie erst den Ordner **[Computer Configuration (Computerkonfiguration)]** oder **[User Configuration (Benutzerkonfiguration)]** und dann die Ordner **[Administrative Templates (Administrative Vorlagen)]**, **[Windows Components (Windows-Komponenten)]** und **[Terminal Services (Terminaldienste)]** erweitern.

Allgemeine Gruppenrichtlinieneinstellungen für Terminaldienste

Zu den allgemeinen Gruppenrichtlinien für Terminaldienste gehören Einstellungen, die das Verhalten bei Anmeldung und Abmeldung, Remote-Sitzungen und das Desktop-Aussehen steuern.

In Tabelle 8-19 werden die Terminaldienste-Gruppenrichtlinieneinstellungen für die Computerkonfiguration beschrieben, die Sie zum Verwalten von View-Desktops verwenden können.

Tabelle 8-19. Allgemeine Richtlinieneinstellungen für Terminaldienste

Einstellung	Beschreibung
`Enforce Removal of Remote Desktop Wallpaper (Entfernen des Remotedesktophintergrunds erzwingen)`	Bei Aktivierung dieser Einstellung wird das Entfernen des Remote-Desktop-Hintergrunds während einer Remote-Sitzung erzwungen, wodurch bei Verbindungen mit niedriger Bandbreite das Benutzererlebnis verbessert wird.
`Limit maximum color depth (Maximale Farbtiefe einschränken)`	Bei Aktivierung dieser Einstellung können Sie die Farbtiefe für View-Desktop-Sitzungen festlegen.

Tabelle 8-19. Allgemeine Richtlinieneinstellungen für Terminaldienste (Fortsetzung)

Einstellung	Beschreibung
Allow users to connect remotely using Terminal Services (Remoteverbindungen für Benutzer mithilfe der Terminaldienste zulassen)	Bei Aktivierung dieser Einstellung können Benutzer eine Remote-Verbindung zum Zielcomputer herstellen.
Remove Windows Security item from Start Menu (Eintrag " Windows-Sicherheit" aus dem Startmenü entfernen)	Bei Deaktivierung dieser Einstellung wird das Element **[Windows Security (Windows-Sicherheit)]** im Einstellungsmenü angezeigt, sodass Benutzer eine Möglichkeit zur Abmeldung erhalten.
Remove Disconnect option from Shut Down dialog (Element "Trennen" aus dem Dialog "Herunterfahren" entfernen)	Bei Aktivierung dieser Einstellung wird die Option **[Disconnect (Trennen)]** aus dem Dialogfeld **[Shut Down Windows (Windows herunterfahren)]** entfernt, sodass weniger Benutzer die Verbindung trennen und sich stattdessen abmelden.

Terminaldienste-Gruppenrichtlinieneinstellungen für Sitzungen

Terminaldienste-Gruppenrichtlinieneinstellungen für Sitzungen umfassen Einstellungen, die getrennte Clientsitzungen und Clientsitzungen im Leerlauf steuern.

Tabelle 8-20 beschreibt die Terminaldienste-Gruppenrichtlinieneinstellungen für die Computerkonfiguration und die Benutzerkonfiguration, die Sie zum Verwalten sitzungsbezogener Eigenschaften für View-Desktops und -Benutzer verwenden können.

Tabelle 8-20. Terminaldienste-Richtlinieneinstellungen für Sitzungen

Einstellung	Beschreibung
Set time limit for disconnected sessions (Zeitlimit für getrennte Sitzungen festlegen)	Wenn Sie diese Einstellung aktivieren, können Sie ein Zeitlimit für getrennte Sitzungen festlegen. Getrennte Sitzungen werden nach Ablauf des festgelegten Zeitlimits abgemeldet.
Set time limit for active but idle Terminal Services sessions (Zeitlimit für aktive, aber im Leerlauf befindliche Terminaldienstesitzungen festlegen)	Wenn Sie diese Einstellung aktivieren, können Sie ein Zeitlimit für im Leerlauf befindliche Sitzungen festlegen. Sitzungen im Leerlauf werden nach Ablauf des festgelegten Zeitlimits abgemeldet.

Sie können diese Einstellungen mit Betriebsrichtlinien für View-Desktops kombinieren, um eine dynamische Lösung für das Anhalten oder Ausschalten getrennter View-Desktop zu erhalten. Durch das Anhalten oder Ausschalten von View-Desktops werden Ressourcen für andere Desktops zur Verfügung gestellt.

Beispiel einer Active Directory-Gruppenrichtlinie

Eine Möglichkeit zur Implementierung von Active Directory-Gruppenrichtlinien in View besteht darin, eine Organisationseinheit (Organizational Unit, OU) für Ihre View-Desktops zu erstellen und mindestens ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) mit dieser OU zu verknüpfen. Sie können mithilfe dieser GPOs Gruppenrichtlinieneinstellungen auf Ihre View-Desktops anwenden und die Loopback-Verarbeitung aktivieren.

Sie können Richtlinien auf Ihrem Active Directory-Server oder einem beliebigen anderen Computer in Ihrer Domäne konfigurieren. Dieses Beispiel zeigt, wie Sie Richtlinien direkt auf Ihrem Active Directory-Server konfigurieren.

Hinweis Da jede View-Umgebung anders ist, müssen Sie möglicherweise unterschiedliche Schritte ausführen, um die Anforderungen der jeweiligen Organisation zu erfüllen.

Vorgehensweise

1 Erstellen einer OU für View-Desktops auf Seite 206

Um Gruppenrichtlinien auf View-Desktops anzuwenden, ohne dass sich dies auf andere Windows-Computer in derselben Active Directory-Domäne auswirkt, erstellen Sie eine Organisationseinheit (Organization Unit, OU) speziell für Ihre View-Desktops.

2 Erstellen von GPOs für View-Gruppenrichtlinien auf Seite 207

Erstellen Sie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) für Gruppenrichtlinien, die Sie für View Manager-Komponenten und den standortbasierten Druck konfigurieren, und verknüpfen Sie diese GPOs anschließend mit der Organisationseinheit (Organizational Unit, OU) für Ihre View-Desktops.

3 Hinzufügen von View-ADM-Vorlagen zu einem GPO auf Seite 207

Um Gruppenrichtlinieneinstellungen für View-Komponenten auf Ihre View-Desktops anzuwenden, fügen Sie die zugehörigen ADM-Vorlagendateien zu GPOs hinzu.

4 Aktivieren der Loopback-Verarbeitung für View-Desktops auf Seite 208

Um Benutzerkonfigurationseinstellungen, die normalerweise für einen Computer gelten, auf alle Benutzer anzuwenden, die sich an diesem Computer anmelden, aktivieren Sie die Loopback-Verarbeitung.

Erstellen einer OU für View-Desktops

Um Gruppenrichtlinien auf View-Desktops anzuwenden, ohne dass sich dies auf andere Windows-Computer in derselben Active Directory-Domäne auswirkt, erstellen Sie eine Organisationseinheit (Organization Unit, OU) speziell für Ihre View-Desktops.

Vorgehensweise

1 Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die Domäne, die Ihre View-Desktops enthält, und wählen Sie **[New (Neu)] > [Organizational Unit (Organisationseinheit)]** .

3 Geben Sie einen Namen für die OU ein und klicken Sie auf **[OK]** .

Die neue OU wird im linken Fensterbereich angezeigt.

4 So fügen Sie der neuen OU View-Desktops hinzu:

a Klicken Sie im linken Fensterbereich auf **[Computers (Computer)]** .

Alle Computerobjekte in der Domäne werden im rechten Fensterbereich angezeigt.

b Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf das Computerobjekt, das den View-Desktop repräsentiert, und wählen Sie **[Move (Verschieben)]** .

c Wählen Sie die OU und klicken Sie auf **[OK]** .

Der View-Desktop wird im rechten Fensterbereich angezeigt, wenn Sie die OU auswählen.

Weiter

Erstellen Sie GPOs für View-Gruppenrichtlinien.

Erstellen von GPOs für View-Gruppenrichtlinien

Erstellen Sie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) für Gruppenrichtlinien, die Sie für View Manager-Komponenten und den standortbasierten Druck konfigurieren, und verknüpfen Sie diese GPOs anschließend mit der Organisationseinheit (Organizational Unit, OU) für Ihre View-Desktops.

Voraussetzungen

- Erstellen Sie eine OU für Ihre View-Desktops.
- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server zur Verfügung stehen.

Vorgehensweise

1. Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .
2. Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Desktops enthält, und wählen Sie **[Properties (Eigenschaften)]** .
3. Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.
4. Klicken Sie mit der rechten Maustaste auf die OU und wählen Sie **[Create and Link a GPO Here (Gruppenrichtlinienobjekt hier erstellen und verknüpfen)]** .
5. Geben Sie einen Namen für das GPO ein und klicken Sie auf **[OK]** .

   Das neue GPO wird im linken Fensterbereich unterhalb der OU angezeigt.
6. (Optional) So wenden Sie das GPO nur auf bestimmte View-Desktops in der OU an:
   a. Wählen Sie das GPO im linken Fensterbereich aus.
   b. Wählen Sie **[Security Filtering (Sicherheitsfilterung)] > [Add (Hinzufügen)]** .
   c. Geben Sie die Computernamen der View-Desktops ein und klicken Sie auf **[OK]** .

      Die View-Desktops werden im Fensterbereich **[Security Filtering (Sicherheitsfilterung)]** angezeigt. Die Einstellungen im GPO werden nur auf diese View-Desktops angewendet.

Weiter

Fügen Sie die View-ADM-Vorlagen zum GPO für Gruppenrichtlinien hinzu.

Hinzufügen von View-ADM-Vorlagen zu einem GPO

Um Gruppenrichtlinieneinstellungen für View-Komponenten auf Ihre View-Desktops anzuwenden, fügen Sie die zugehörigen ADM-Vorlagendateien zu GPOs hinzu.

Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für View-Komponenten und verknüpfen Sie sie mit der Organisationseinheit (Organizational Unit, OU), die Ihre View-Desktops enthält.
- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server zur Verfügung stehen.

Vorgehensweise

1 Kopieren Sie die ADM-Vorlagendateien für View aus dem Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\extras\GroupPolicyFiles auf Ihrem View Connection Server-Host auf Ihren Active Directory-Server.

2 Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

3 Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Desktops enthält, und wählen Sie **[Properties (Eigenschaften)]** .

4 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

5 Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **[Edit (Bearbeiten)]** .

Das Fenster Group Policy Object Editor (Gruppenrichtlinienobjekt-Editor) wird angezeigt.

6 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste unter **[Computer Configuration (Computerkonfiguration)]** auf **[Administrative Templates (Administrative Vorlagen)]** und wählen Sie **[Add/Remove Templates (Vorlagen hinzufügen/entfernen)]** .

7 Klicken Sie auf **[Add (Hinzufügen)]** , suchen Sie nach der ADM-Vorlagendatei, und klicken Sie auf **[Open (Öffnen)]** .

8 Klicken Sie auf **[Close (Schließen)]** , um die Richtlinieneinstellungen in der ADM-Vorlagendatei auf das GPO anzuwenden.

Der Name der Vorlage erscheint im linken Fensterbereich unterhalb von **[Administrative Templates (Administrative Vorlagen)]** .

9 Konfigurieren Sie die Gruppenrichtlinieneinstellungen.

Weiter

Aktivieren Sie die Loopback-Verarbeitung für Ihre View-Desktops.

Aktivieren der Loopback-Verarbeitung für View-Desktops

Um Benutzerkonfigurationseinstellungen, die normalerweise für einen Computer gelten, auf alle Benutzer anzuwenden, die sich an diesem Computer anmelden, aktivieren Sie die Loopback-Verarbeitung.

Voraussetzungen

- Erstellen Sie GPOs für die Gruppenrichtlinieneinstellungen für View-Komponenten und verknüpfen Sie sie mit der Organisationseinheit (Organizational Unit, OU), die Ihre View-Desktops enthält.
- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server zur Verfügung stehen.

Vorgehensweise

1 Wählen Sie auf Ihrem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die OU, die Ihre View-Desktops enthält, und wählen Sie **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **[Edit (Bearbeiten)]** .

Das Fenster Group Policy Object Editor (Gruppenrichtlinienobjekt-Editor) wird angezeigt.

5 Erweitern Sie den Ordner **[Computer Configuration (Computerkonfiguration)]** und anschließend die Ordner **[Administrative Templates (Administrative Vorlagen)]** , **[System]** und **[Group Policy (Gruppenrichtlinie)]** .

6 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf **[User Group Policy loopback processing mode (Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie)]** und wählen Sie **[Properties (Eigenschaften)]** .

7 Wählen Sie auf der Registerkarte **[Setting (Einstellung)]** die Option **[Enabled (Aktiviert)]** und wählen Sie anschließend im Dropdown-Menü **[Mode (Modus)]** den Modus zur Loopback-Verarbeitung aus.

Option	Aktion
Merge (Zusammenführen)	Die angewendeten Benutzerrichtlinieneinstellungen sind eine Kombination der Richtlinien in den Computer- und Benutzer-GPOs. Bei Konflikten haben die Computer-GPOs Vorrang.
Replace (Ersetzen)	Die Benutzerrichtlinie wird ausschließlich anhand der mit dem Computer verknüpften GPOs definiert. Mit dem Benutzer verknüpfte GPOs werden ignoriert.

8 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Konfigurieren von Benutzerprofilen mit View Persona-Verwaltung 9

Mit View Persona-Verwaltung können Sie Benutzerprofile konfigurieren, die dynamisch mit einem Remote-Profil-Repository synchronisiert werden. Diese Funktion gibt Benutzern Zugriff auf eine persönliche Desktop-Erfahrung bei jeder Desktop-Anmeldung. View Persona-Verwaltung erweitert die Funktionalität und verbessert die Leistung von servergespeicherten Windows-Profilen.

Sie konfigurieren Gruppenrichtlinieneinstellungen, um View Persona-Verwaltung zu aktivieren und verschiedene Aspekte Ihrer View Persona-Verwaltung-Bereitstellung zu steuern.

Um View Persona-Verwaltung zu aktivieren und zu verwenden, müssen Sie eine View Premier-Lizenz haben. Siehe VMware-Endbenutzerlizenzvereinbarung (EULA) unter http://www.vmware.com/de/download/eula.

Dieses Kapitel behandelt die folgenden Themen:

- „Bereitstellen von Benutzerpersonas in View“, auf Seite 211
- „Persona-Verwaltung und servergespeicherte Windows-Profile“, auf Seite 212
- „Konfigurieren einer View Persona-Verwaltung-Bereitstellung“, auf Seite 212
- „Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona-Verwaltung-Bereitstellung“, auf Seite 220
- „Gruppenrichtlinieneinstellungen für View Persona-Verwaltung“, auf Seite 223

Bereitstellen von Benutzerpersonas in View

Mit der View Persona-Verwaltung-Funktion wird das Remote-Profil eines Benutzers automatisch heruntergeladen, wenn sich der Benutzer bei einem View-Desktop anmeldet. Sie können View für das Speichern von Benutzerprofilen in einem sicheren, zentralisierten Repository konfigurieren. View lädt Persona-Informationen herunter, wenn der Benutzer sie benötigt.

View Persona-Verwaltung ist eine Alternative zu servergespeicherten Windows-Profilen. View Persona-Verwaltung erweitert die Funktionalität und verbessert die Leistung im Vergleich zu servergespeicherten Windows-Profilen.

Sie können mit View alle Aspekte von Personas konfigurieren und verwalten. Es ist nicht erforderlich, servergespeicherte Windows-Profile zu konfigurieren. Wenn Sie eine Konfiguration mit servergespeicherten Windows-Profilen verwenden, können Sie die vorhandene Repository-Konfiguration mit View verwenden.

Ein Benutzerprofil ist unabhängig vom virtuellen Desktop. Wenn sich ein Benutzer an einem beliebigen Desktop anmeldet, wird dasselbe Profil angezeigt.

Beispielsweise kann sich der Benutzer an einem Linked-Clone-Desktop-Pool mit dynamischer Zuweisung anmelden und den Desktop-Hintergrund und die Microsoft Word-Einstellungen ändern. Wenn der Benutzer die nächste Sitzung startet, wird eine andere virtuelle Maschine verwendet, der Benutzer sieht jedoch dieselben Einstellungen.

Ein Benutzerprofil umfasst verschiedene, vom Benutzer generierte Informationen:

- Benutzerspezifische Daten und Desktop-Einstellungen
- Anwendungsdaten und -einstellungen
- Von Benutzeranwendungen konfigurierte Windows-Registrierungseinträge

Wenn Sie Desktops mit ThinApp-Anwendungen bereitstellen, können die ThinApp Sandbox-Daten ebenfalls im Benutzerprofil gespeichert und dem Benutzer bei Bedarf zur Verfügung gestellt werden.

View Persona-Verwaltung minimiert die Zeit, die zum An- und Abmelden von Desktops aufgebracht werden muss. Die An- und Abmeldedauer kann bei servergespeicherten Windows-Profilen zu einem Problem werden.

- Während der Anmeldung lädt View nur die für Windows erforderlichen Dateien herunter, beispielsweise die Benutzerregistrierungsdateien. Andere Dateien werden auf den lokalen Desktop kopiert, wenn der Benutzer oder eine Anwendung sie vom lokalen Profilordner aus öffnet.
- View kopiert kürzlich vorgenommene Änderungen am lokalen Profil in das Remote-Repository, im Normalfall alle paar Minuten. Der Standardwert lautet alle 10 Minuten. Sie können festlegen, wie oft das lokale Profil hochgeladen werden soll.
- Beim Abmelden werden nur solche Dateien, die seit der letzten Änderung aktualisiert wurden, in das Remote-Repository kopiert.

Persona-Verwaltung und servergespeicherte Windows-Profile

Wenn Persona-Verwaltung aktiviert ist, können Sie die Personas der View-Benutzer nicht mit den servergespeicherten Windows-Profilen verwalten.

Wenn Sie sich z. B. beim Gastbetriebssystem eines Desktops anmelden, zur Registerkarte **[Advanced (Erweitert)]** im Dialogfeld „System Properties (Systemeigenschaften)“ navigieren und die Benutzerprofileinstellungen von **[Roaming profile (Servergespeichertes Profil)]** in **[Local profile (Lokales Profil)]** ändern, synchronisiert View Persona-Verwaltung die Benutzerpersonas weiterhin zwischen dem lokalen Desktop und dem Remote-Persona-Repository.

Sie können jedoch Dateien und Ordner innerhalb von Benutzer-Personas angeben, die von servergespeicherte Windows-Profilen statt von View Persona-Verwaltung verwaltet werden. Sie verwenden zum Angeben dieser Dateien und Ordner die Richtlinie **[Windows Roaming Profiles Synchronization (Synchronisierung von servergespeicherten Windows-Profilen]** .

Konfigurieren einer View Persona-Verwaltung-Bereitstellung

Um View Persona-Verwaltung zu konfigurieren, richten Sie ein Remote-Repository ein, in dem Benutzerprofile gespeichert werden, installieren View Agent mit der **[View Persona Management (View Persona-Verwaltung)]** -Einrichtungsoption auf VM-Desktops, fügen View Persona-Verwaltung-Gruppenrichtlinieneinstellungen hinzu und konfigurieren diese, und stellen schließlich Desktop-Pools bereit.

Übersicht über das Einrichten einer View Persona-Verwaltung Bereitstellung

Um eine View-Desktop-Bereitstellung mit View Persona-Verwaltung einzurichten, müssen Sie verschiedene Aufgaben auf hoher Ebene durchführen.

Diese Reihenfolge ist zu empfehlen, obwohl Sie diese Aufgaben auch in anderer Reihenfolge durchführen können. Beispielsweise können Sie Gruppenrichtlinieneinstellungen in Active Directory konfigurieren oder neu konfigurieren, nachdem Sie Desktop-Pools bereitgestellt haben.

1 Konfigurieren Sie ein Remote-Repository zum Speichern der Benutzerprofile.

  Sie können eine Netzwerkfreigabe konfigurieren oder einen vorhandenen Active Directory-Benutzerprofilpfad verwenden, den Sie für servergespeicherte Windows-Profile konfiguriert haben.

2 Installieren Sie View Agent mit der Einrichtungsoption **[View Persona-Verwaltung]** auf virtuellen Maschinen, die Sie zum Erstellen von Desktop-Pools verwenden.

3 Fügen Sie die View Persona-Verwaltung-ADM-Vorlagendatei der „Active Directory Server (Active Directory-Server)“- oder der „Local Computer Policy (Richtlinie für 'Lokaler Computer')“-Konfiguration auf der übergeordneten virtuellen Maschine hinzu.

   Um View Persona-Verwaltung (für Ihre gesamte View-Bereitstellung zu konfigurieren, fügen Sie die ADM-Vorlagendatei zu Active Directory hinzu.

   Um View Persona-Verwaltung einem Desktop-Pool hinzuzufügen, können Sie folgendermaßen vorgehen:

   - Fügen Sie die ADM-Vorlagendatei der virtuelle Maschine hinzu, die Sie zum Erstellen des Pools verwenden.
   - Fügen Sie die ADM-Vorlagendatei zu Active Directory hinzu und wenden Sie die Gruppenrichtlinieneinstellungen auf die OU an, die die Desktops im Pool enthält.

4 Aktivieren Sie View Persona-Verwaltung, indem Sie die Gruppenrichtlinieneinstellung **[Manage user persona (Benutzerpersona verwalten)]** aktivieren.

5 Wenn Sie eine Netzwerkfreigabe für das Remoteprofil-Repository konfiguriert haben, aktivieren Sie die Gruppenrichtlinieneinstellung **[Persona repository location (Speicherort für das Persona-Repository)]**, und geben Sie den Netzwerkfreigabepfad an.

6 (Optional) Konfigurieren Sie die Gruppenrichtlinieneinstellungen in Active Directory oder der Konfiguration für die „Local Computer Policy (Richtlinie für 'Lokaler Computer')“.

7 Erstellen Sie Desktop-Pools aus virtuellen Maschinen, auf denen Sie View Agent mit der Einrichtungsoption **[View Persona-Verwaltung]** installiert haben.

Konfigurieren eines Benutzerprofil-Repositorys

Sie können ein Remote-Repository konfigurieren, um die Benutzerdaten und -einstellungen, anwendungsspezifischen Daten und andere vom Benutzer generierte Informationen in Benutzerprofilen zu speichern. Wenn servergespeicherte Windows-Profile in Ihrer Bereitstellung konfiguriert sind, können Sie stattdessen einen vorhandenen Active Directory-Benutzerprofilpfad verwenden.

Hinweis Sie können View Persona-Verwaltung konfigurieren, ohne servergespeicherte Windows-Profile konfigurieren zu müssen.

Voraussetzungen

Machen Sie sich mit den Richtlinien zum Erstellen eines Benutzerprofil-Repositorys vertraut. Siehe „Erstellen einer Netzwerkfreigabe für View Persona-Verwaltung“, auf Seite 214.

Vorgehensweise

1 Bestimmen Sie, ob Sie einen vorhandenen Active Directory-Benutzerprofilpfad verwenden oder ein Benutzerprofil-Repository auf einer Netzwerkfreigabe konfigurieren möchten.

Option	Aktion
Verwenden Sie einen vorhandenen Active Directory-Benutzerprofilpfad	Wenn Sie über eine vorhandene Konfiguration servergespeicherter Windows-Profile verfügen, können Sie den in Active Directory angegebenen Benutzerprofilpfad verwenden, der servergespeicherte Profile unterstützt. Sie können die übrigen Schritte in dieser Schrittfolge überspringen.
Konfigurieren einer Netzwerkfreigabe zur Speicherung des Persona-Repositorys	Wenn Sie keine servergespeicherten Windows-Profile konfiguriert haben, müssen Sie eine Netzwerkfreigabe für das Benutzerprofil-Repository konfigurieren. Befolgen Sie die verbleibenden Schritte in dieser Schrittfolge.

2 Erstellen Sie einen freigegebenen Ordner auf einem Computer, auf den Ihre Benutzer von den Gastbetriebssystemen auf ihren Desktops aus zugreifen können.

   Wenn `%Benutzername%` nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona-Verwaltung `%Benutzername%.%Benutzerdomäne%` an den Pfad an.

   Beispiel: `\\server.domain.com\VPRepository\%Benutzername%.%Benutzerdomäne%`

3 Legen Sie Zugriffsberechtigungen für die Ordnerfreigaben fest, die Benutzerprofile enthalten.

   Legen Sie die Berechtigungen fest, die Sie zum Konfigurieren der Sicherheit für servergespeicherte Windows-Profile verwenden möchten. Details finden Sie im Microsoft TechNet-Thema *Security Recommendations for Roaming User Profiles Shared Folders*.
   http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx

Erstellen einer Netzwerkfreigabe für View Persona-Verwaltung

Sie müssen bestimmte Richtlinien befolgen, wenn Sie einen freigegebenen Ordner erstellen, der als Profil-Repository verwendet werden soll.

- Sie erstellen den freigegebenen Ordner auf einem Server, einem NAS-Gerät (Network-Attached Storage) oder einem Netzwerkserver.
- Der freigegebene Ordner muss sich nicht in derselben Domäne befinden wie View Connection Server.
- Der freigegebene Ordner muss sich in derselben Active Directory-Ordnerstruktur befinden wie die Benutzer, die Profile im freigegebenen Ordner speichern.
- Sie müssen ein freigegebenes Laufwerk verwenden, das groß genug ist, um die Benutzerprofilinformationen für Ihre Benutzer zu speichern. Zum Unterstützen einer großen View-Bereitstellung können Sie separate Repositories für verschiedene Desktop-Pools konfigurieren.

  Wenn Benutzer zu mehr als einem Pool berechtigt sind, müssen die Pools mit gemeinsamen Benutzern im selben Profil-Repository konfiguriert sein. Wenn Sie einen Benutzer zu zwei Pools mit verschiedenen Profil-Repositorys berechtigen, kann der Benutzer von Desktops in jedem Pool nicht auf dieselbe Version des Profils zugreifen.
- Sie müssen den vollständigen Profilpfad erstellen, unter dem die Benutzerprofilordner erstellt werden. Wenn der Pfad unvollständig ist, erstellt Windows die fehlenden Ordner, wenn sich der erste Benutzer anmeldet und die Sicherheitsbeschränkungen des Benutzers auf diese Ordner zuweist. Windows weist allen unter dem Pfad erstellten Ordnern dieselben Sicherheitsbeschränkungen zu.

  Für `Benutzer1` könnten Sie beispielsweise den View Persona-Verwaltung-Pfad `\\server\VPRepository\profiles\Benutzer1` konfigurieren. Wenn Sie die Netzwerkfreigabe `\\server\VPRepository` erstellen und der Ordner `profiles` nicht vorhanden ist, erstellt Windows den Pfad `\profiles\Benutzer1`, wenn sich `Benutzer1` anmeldet. Windows beschränkt den Zugriff auf die Ordner `\profiles\Benutzer1` auf das Konto `Benutzer1`. Wenn sich ein anderer Benutzer mit einem Profilpfad in `\\server\VPRepository\profiles` anmeldet, kann der zweite Benutzer nicht auf das Repository zugreifen, und das Benutzerprofil wird nicht repliziert.

Installieren von View Agent mit der View Persona-Verwaltung-Option

Zum Verwenden von View Persona-Verwaltung mit View-Desktops müssen Sie View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** auf den virtuellen Maschinen installieren, die Sie zum Erstellen von Desktop-Pools verwenden.

Für einen automatisierten Pool installieren Sie View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** auf der virtuellen Maschine, die Sie als übergeordnetes Element oder als Vorlage verwenden. Wenn Sie einen Desktop-Pool von der virtuellen Maschine aus erstellen, wird die View Persona-Verwaltung-Software auf Ihren View-Desktops bereitgestellt.

Für einen manuellen Pool müssen Sie View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** auf jeder virtuellen Maschine installieren, die als Desktop-Quelle im Pool verwendet wird. Verwenden Sie Active Directory, um View Persona-Verwaltung-Gruppenrichtlinien für einen manuellen Pool zu konfigurieren. Alternativ können Sie auch auf jeder einzelnen Desktop-Quelle die ADM-Vorlagendatei hinzufügen und Gruppenrichtlinien konfigurieren.

Hinweis Ein Benutzer kann nicht auf dasselbe Profil zugreifen, wenn der Benutzer zwischen Desktops wechselt, die die Benutzerprofile „v1“ und „v2“ haben. Windows XP verwendet v1-Profile. Windows Vista und Windows 7 verwenden v2-Profile.

Wenn sich ein Benutzer beispielsweise bei einem Windows XP-Desktop und später bei einem Windows 7-Desktop anmeldet, kann die virtuelle Windows 7-Maschine das v1-Profil nicht lesen, das während der Windows XP-Desktopsitzung erstellt wurde.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Installation auf einer virtuellen Maschine mit Windows 7, Windows Vista oder Windows XP durchführen. View Persona Management funktioniert nicht auf physischen Computern oder Microsoft-Terminalservern.
- Stellen Sie sicher, dass Sie sich als Administrator auf der virtuellen Maschine anmelden können.
- Stellen Sie sicher, dass kein natives RTO Virtual Profile 2.0 auf der virtuellen Maschine installiert ist. Wenn ein natives RTO Virtual Profile 2.0 vorhanden ist, deinstallieren Sie es, bevor Sie View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** installieren.
- Laden Sie auf virtuellen Maschinen mit Windows XP das Dienstprogramm Microsoft User Profile Hive Cleanup Service (UPHClean) herunter und installieren Sie dieses im Gastbetriebssystem. Siehe „Installieren von UPHClean auf Windows XP-Desktops, die View Persona-Verwaltung verwenden“, auf Seite 215.
- Machen Sie sich mit dem Installieren von View Agent vertraut. Siehe „Installieren von View Agent auf einer virtuellen Maschine“, auf Seite 57 oder „Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle“, auf Seite 48.

Vorgehensweise

- Wenn Sie View Agent auf einer virtuellen Maschine installieren, wählen Sie die Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** aus.

Weiter

Fügen Sie die View Persona Management-ADM-Vorlagendatei der „Active Directory Server (Active Directory-Server)“- oder der „Local Computer Policy (Richtlinie für 'Lokaler Computer')“-Konfiguration auf der virtuellen Maschine selbst hinzu. Siehe „Hinzufügen der View Persona-Verwaltung-ADM-Vorlagendatei“, auf Seite 216.

Installieren von UPHClean auf Windows XP-Desktops, die View Persona-Verwaltung verwenden

Der Microsoft User Profile Hive Cleanup Service (UPHClean) stellt sicher, dass Benutzersitzungen vollständig getrennt werden, wenn sich ein Benutzer abmeldet. UPHClean bereinigt Registrierungsschlüssel-Handles, die sonst von anderen Vorgängen oder Anwendungen freigelegt werden könnten. Dieser Service hilft dabei sicherzustellen, dass die Registry-Struktur des Benutzers entladen wird, damit diese erfolgreich hochgeladen und die lokale Persona gelöscht werden kann.

Wenn Sie View Persona-Verwaltung auf virtuellen Windows XP-Maschinen konfigurieren, laden Sie UPHClean in das Gastbetriebssystem herunter und installieren Sie den Dienst.

Sie können den UPHClean-Dienst von folgendem Speicherort herunterladen: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6676.

Der UPHClean-Dienst ist in die Betriebssysteme Windows 7 und Windows Vista integriert. Unter diesen Betriebssystemen müssen Sie den Dienst nicht installieren.

Hinzufügen der View Persona-Verwaltung-ADM-Vorlagendatei

Die View Persona-Verwaltung-ADM-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, mit denen Sie View Persona-Verwaltung konfigurieren können. Bevor Sie die Richtlinien konfigurieren können, müssen Sie die ADM-Vorlagendatei den lokalen virtuellen Maschinen oder dem Active Directory-Server hinzufügen.

Um View Persona-Verwaltung auf einer einzelnen virtuellen Maschine zu konfigurieren, können Sie die Gruppenrichtlinieneinstellungen der Konfiguration „Local Computer Policy (Richtlinie für 'Lokaler Computer')“ auf dem lokalen System hinzufügen.

Zum Konfigurieren von View Persona-Verwaltung für einen Desktop-Pool können Sie die Gruppenrichtlinieneinstellungen der Richtlinie „Local Computer Policy (Richtlinie für 'Lokaler Computer')“ auf der virtuellen Maschine hinzufügen, die Sie als übergeordnetes Element oder Vorlage zum Bereitstellen des Desktop-Pools verwenden.

Zum Konfigurieren von View Persona-Verwaltung auf der domänenweiten Ebene und zum Anwenden der Konfiguration auf viele Desktops oder Ihre gesamte Bereitstellung können Sie die Gruppenrichtlinieneinstellungen den GPOs (Group Policy Objects, Gruppenrichtlinienobjekten) auf Ihrem Active Directory-Server hinzufügen. In Active Directory können Sie eine OU für die Desktops erstellen, die View Persona-Verwaltung verwenden, ein oder mehrere GPOs erstellen und die GPOs mit der OU verknüpfen. Um separate View Persona-Verwaltung-Richtlinien für unterschiedliche Benutzertypen zu konfigurieren, können Sie OUs für bestimmte Desktopsets erstellen und verschiedene GPOs auf die OUs anwenden.

Ein Beispiel für das Implementieren von Active Directory-Gruppenrichtlinien in View finden Sie unter „Beispiel einer Active Directory-Gruppenrichtlinie“, auf Seite 205.

Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem

Um View Persona-Verwaltung für einen einzelnen Desktop-Pool zu konfigurieren, fügen Sie die Persona-Verwaltung-ADM-Vorlagendatei zur Richtlinie für den lokalen Computer auf der virtuellen Maschine hinzu, die Sie zum Erstellen des Pools verwenden. Um View Persona-Verwaltung für ein einzelnes System zu konfigurieren, müssen Sie diesem System die Persona-Verwaltung-ADM-Vorlagendatei hinzufügen.

Voraussetzungen

- Stellen Sie, dass View Agent mit der View Persona-Verwaltung-Einrichtungsoption auf dem System installiert ist. Siehe „Installieren von View Agent mit der View Persona-Verwaltung-Option“, auf Seite 214.
- Stellen Sie sicher, dass Sie sich als Administrator beim System anmelden können.

Vorgehensweise

1 Klicken Sie auf dem lokalen System auf **[Start]** > **[Run (Ausführen)]** .

2 Geben Sie **`gpedit.msc`** ein und klicken Sie auf **[OK]** .

3 Navigieren Sie im Fenster Local Computer Policy (Richtlinie für 'Lokaler Computer') zu **[Computer Configuration (Computerkonfiguration)]** und klicken Sie mit der rechten Maustaste auf **[Administrative Templates (Administrative Vorlagen)]** .

HINWEIS Wählen Sie **[Administrative Templates (Administrative Vorlagen)]** unter **[User Configuration (Benutzerkonfiguration)]** nicht aus.

---

4 Klicken Sie auf **[Add/Remove Templates (Vorlagen hinzufügen/entfernen)]** und dann auf **[Add (Hinzufügen)]** .

5 Gehen Sie zum Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Agent\bin.

Die ADM-Vorlagendatei `ViewPM.adm` befindet sich in diesem Verzeichnis.

Die Datei `ViewPM.adm` ist zusammen mit den anderen View ADM-Vorlagendateien auch im Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\extras\GroupPolicyFiles auf dem View Connection Server-Host installiert.

6 Wählen Sie die Datei `ViewPM.adm` und klicken Sie dann auf **[Add (Hinzufügen)]** .

7 Schließen Sie das Fenster Add/Remove Templates (Vorlagen hinzufügen/entfernen).

Die Gruppenrichtlinieneinstellungen für View Persona-Verwaltung werden der Konfiguration „Local Computer Policy (Richtlinie für 'Lokaler Computer')“ auf dem lokalen System hinzugefügt. Sie müssen `gpedit.msc` verwenden, um diese Konfiguration anzuzeigen.

Weiter

Konfigurieren Sie die Gruppenrichtlinieneinstellungen für View Persona-Verwaltung auf dem lokalen System. Siehe „Konfigurieren von View Persona-Verwaltung-Richtlinien“, auf Seite 218.

Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu Active Directory

Um View Persona-Verwaltung für Ihre Bereitstellung zu konfigurieren, können Sie die View Persona-Verwaltung-ADM-Vorlagendatei zu einem Gruppenrichtlinienobjekt (GPO) auf Ihrem Active Directory-Server hinzufügen.

Voraussetzungen

- Erstellen Sie Gruppenrichtlinienobjekte für Ihre View Persona-Verwaltung-Bereitstellung und verknüpfen Sie sie mit der OU, die die View-Desktops enthält, welche View Persona-Verwaltung verwenden. Siehe „Beispiel einer Active Directory-Gruppenrichtlinie“, auf Seite 205.
- Stellen Sie sicher, dass die Microsoft Management Console (MMC) und der Gruppenrichtlinienobjekt-Editor auf Ihrem Active Directory-Server zur Verfügung stehen.
- Stellen Sie sicher, dass View Agent mit der View Persona-Verwaltung-Einrichtungsoption auf einem System installiert ist, auf das von Ihrem Active Directory-Server aus zugegriffen werden kann. Siehe „Installieren von View Agent mit der View Persona-Verwaltung-Option“, auf Seite 214.

Vorgehensweise

1 Kopieren Sie die View Persona-Verwaltung-ADM-Vorlagendatei, `ViewPM.adm`, auf Ihren Active Directory-Server.

Die Datei `ViewPM.adm` befindet sich im Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\extras\GroupPolicyFiles auf dem View Connection Server-Host.

2 Öffnen Sie auf Ihrem Active Directory-Server die Verwaltungskonsole für Gruppenrichtlinien.

Rufen Sie z. B. das Dialogfeld „Run (Ausführen)“ auf, geben Sie **`gpmc.msc`** ein und klicken Sie auf **[OK]** .

3 Wählen Sie im linken Fensterbereich die Domäne oder die OU aus, die Ihre View-Desktops enthält.

4 Klicken Sie im rechten Fensterbereich auf das GPO, das Sie für die Gruppenrichtlinieneinstellungen erstellt haben, und wählen Sie **[Edit (Bearbeiten)]** .

Das Fenster Group Policy Object Editor (Gruppenrichtlinienobjekt-Editor) wird angezeigt.

5 Klicken Sie im Gruppenrichtlinienobjekt-Editor mit der rechten Maustaste unter **[Computer Configuration (Computerkonfiguration)]** auf **[Administrative Templates (Administrative Vorlagen)]** und wählen Sie **[Add/Remove Templates (Vorlagen hinzufügen/entfernen)]** .

6 Klicken Sie auf **[Add (Hinzufügen)]**, suchen Sie nach der Datei `ViewPM.adm` und klicken Sie auf **[Open (Öffnen)]**.

7 Klicken Sie auf **[Close (Schließen)]**, um die Richtlinieneinstellungen in der ADM-Vorlagendatei auf das GPO anzuwenden.

Der Name der Vorlage erscheint im linken Fensterbereich unterhalb von **[Administrative Templates (Administrative Vorlagen)]**.

Weiter

Konfigurieren Sie die Gruppenrichtlinieneinstellungen für View Persona-Verwaltung auf Ihrem Active Directory-Server.

Konfigurieren von View Persona-Verwaltung-Richtlinien

Um View Persona-Verwaltung zu verwenden, müssen Sie die Gruppenrichtlinieneinstellung **[Manage user persona (Benutzerpersona verwalten)]** aktivieren, wodurch die View Persona-Verwaltung-Software aktiviert wird. Um ein Benutzerprofil-Repository ohne Verwendung eines Active Directory-Benutzerprofilpfades einzurichten, müssen Sie die Gruppenrichtlinieneinstellung **[Persona repository location (Speicherort für das Persona-Repository)]** konfigurieren.

Sie können die optionalen Gruppenrichtlinieneinstellungen konfigurieren, um andere Aspekte Ihrer View Persona-Verwaltung-Bereitstellung zu konfigurieren.

Wenn servergespeicherte Windows-Profile bereits in Ihrer Bereitstellung konfiguriert sind, können Sie einen vorhandenen Active Directory-Benutzerprofilpfad verwenden. Sie können die Einstellung **[Persona repository location (Speicherort für das Persona-Repository)]** deaktiviert oder nicht konfiguriert lassen.

Voraussetzungen

- Machen Sie sich mit den Gruppenrichtlinieneinstellungen **[Manage user persona (Benutzerpersona verwalten)]** und **[Persona repository location (Speicherort für das Persona-Repository)]** vertraut. Siehe „Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung“, auf Seite 225.
- Wenn Sie Gruppenrichtlinien auf einem lokalen System einrichten, machen Sie sich mit dem Öffnen des Fensters „Group Policy (Gruppenrichtlinie)“ vertraut. Siehe Schritte Schritt 1 und Schritt 2 in „Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem“, auf Seite 216.
- Wenn Sie auf Ihrem Active Directory-Server Gruppenrichtlinien festlegen, machen Sie sich mit dem Editor für Gruppenrichtlinienobjekte vertraut. Siehe Schritte Schritt 2 bis Schritt 4 in „Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu Active Directory“, auf Seite 217.

Vorgehensweise

1 Öffnen Sie das Fenster „Group Policy (Gruppenrichtlinie)“.

Option	Beschreibung
Local system (Lokales System)	Öffnet das Fenster „Local Computer Policy (Richtlinie für 'Lokaler Computer')“.
Active Directory Server (Active Directory-Server)	Öffnet das Fenster „Group Policy Object Editor (GPO-Editor)“.

2 Erweitern Sie den Ordner **[Computer Configuration (Computerkonfiguration)]**, und navigieren Sie zum Ordner **[Persona Management (Persona-Verwaltung)]**.

Option	Beschreibung
Windows XP oder Windows Server 2003	Erweitern Sie die folgenden Ordner: **[Administrative Templates (Administrative Vorlagen)]**, **[VMware View Agent Configuration (VMware View Agent-Konfiguration)]**, **[Persona Management (Persona-Verwaltung)]**
Windows Vista und höher oder Windows Server 2008 und höher	Erweitern Sie die folgenden Ordner: **[Administrative Templates (Administrative Vorlagen)]**, **[Classic Administrative Templates (ADM) (Klassische administrative Vorlagen (ADM))]**, **[VMware View Agent Configuration (VMware View Agent-Konfiguration)]**, **[Persona Management (Persona-Verwaltung)]**

3 Öffnen Sie den Ordner **[Roaming& Synchronization (Servergespeichert &Synchronisierung)]**.

4 Doppelklicken Sie auf **[Manage user persona (Benutzerpersona verwalten)]**, und klicken Sie auf **[Enabled (Aktiviert)]**.

Diese Einstellung aktiviert View Persona-Verwaltung. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, funktioniert View Persona-Verwaltung nicht.

5 Geben Sie das Profiluploadintervall in Minuten ein, und klicken Sie auf **[OK]**.

Das Profiluploadintervall bestimmt, wie oft View Persona-Verwaltung Änderungen an den Benutzerprofilen in das Remote-Repository kopiert. Die Standardeinstellung ist 10 Minuten.

6 Doppelklicken Sie auf **[Persona repository location (Speicherort für das Persona-Repository)]**, und klicken Sie dann auf **[Enabled (Aktiviert)]**.

Wenn Sie über eine vorhandene Bereitstellung servergespeicherter Windows-Profile verfügen, können Sie einen Active Directory-Benutzerprofilpfad für das Remote-Profil-Repository verwenden. Sie müssen keinen **[Persona repository location (Speicherort für das Persona-Repository)]** konfigurieren.

7 Geben Sie den UNC-Pfad zu einer Netzwerkdateiserverfreigabe ein, in der die Benutzerprofile gespeichert werden.

Beispiel: `\\server.domain.com\UserProfilesRepository\%Benutzername%`

Die virtuellen Maschinen in Ihrer Bereitstellung müssen auf diese Netzwerkfreigabe zugreifen können.

Wenn Sie vorhaben, einen Active Directory-Benutzerprofilpfad zu verwenden, brauchen Sie keinen UNC-Pfad anzugeben.

8 Wenn ein Active Directory-Benutzerprofilpfad in Ihrer Bereitstellung konfiguriert ist, bestimmen Sie, ob dieser Pfad benutzt oder außer Kraft gesetzt werden soll.

Option	Aktion
Verwenden Sie die Netzwerkfreigabe.	Markieren Sie das Kontrollkästchen **[Override Active Directory user profile path if it is configured (Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist)]**.
Verwenden Sie, falls vorhanden, einen Active Directory-Benutzerprofilpfad.	Markieren Sie das Kontrollkästchen **[Override Active Directory user profile path if it is configured (Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist)]** nicht.

9 Klicken Sie auf **[OK]**.

10 (Optional) Konfigurieren Sie andere Gruppenrichtlinieneinstellungen für View Persona-Verwaltung.

Erstellen von View-Desktops, die Persona-Verwaltung verwenden

Um View Persona-Verwaltung mit View-Desktops zu verwenden, müssen Sie Desktop-Pools mit einem auf jedem Desktop installierten View Persona-Verwaltung-Agenten erstellen.

Sie müssen View Persona-Verwaltung auf virtuellen Maschinen bereitstellen. Sie können View Persona-Verwaltung nicht auf physischen Computern oder Microsoft-Terminalservern verwenden.

Für Desktops, die im lokalen Modus ausgeführt werden, kann View Persona-Verwaltung nicht verwendet werden.

Voraussetzungen

- Stellen Sie sicher, dass der View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** auf der virtuellen Maschine installiert ist, die Sie zum Erstellen des Desktop-Pools verwenden. Siehe „Installieren von View Agent mit der View Persona-Verwaltung-Option“, auf Seite 214.
- Wenn Sie beabsichtigen, View Persona-Verwaltung-Richtlinien nur für diesen Pool zu konfigurieren, stellen Sie sicher, dass Sie die View Persona-Verwaltung-ADM-Vorlagendatei zur virtuellen Maschine hinzugefügt und Gruppenrichtlinieneinstellungen in der Richtlinie „Local Computer Policy“ (Richtlinie für 'Lokaler Computer') konfiguriert haben. Siehe „Hinzufügen der Persona-Verwaltung-ADM-Vorlage zu einem Einzelsystem“, auf Seite 216 und „Konfigurieren von View Persona-Verwaltung-Richtlinien“, auf Seite 218.

Vorgehensweise

- Generieren Sie eine Vorlage oder einen Snapshot der virtuellen Maschine und erstellen Sie einen automatisierten Desktop-Pool.

  Sie können die View Persona-Verwaltung mit Pools konfigurieren, die vollständige virtuelle Maschinen oder Linked-Clone-Desktops enthalten. Die Pools können hierbei eine dedizierte oder eine dynamische Zuweisung verwenden.
- (Optional) Um View Persona-Verwaltung mit manuellen Desktop-Pools zu verwenden, wählen Sie die Desktopquellen aus, auf denen View Agent mit der Option **[View Persona Management (View Persona-Verwaltung)]** installiert ist.

Hinweis Wenn Sie nach der Bereitstellung von View Persona-Verwaltung auf Ihren View-Desktops die Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** auf den Desktops entfernen oder View Agent komplett deinstallieren, werden die lokalen Benutzerprofile von den Desktops der Benutzer entfernt, die aktuell nicht angemeldet sind. Für Benutzer, die aktuell angemeldet sind, werden die Benutzerprofile während des Deinstallationsprozesses vom Remote-Profil-Repository heruntergeladen.

Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona-Verwaltung-Bereitstellung

Sie sollten den empfohlenen Vorgehensweisen für das Konfigurieren von View Persona-Verwaltung folgen, um die Erfahrung Ihrer Desktop-Benutzer zu verbessern und um sicherzustellen, dass View Persona-Verwaltung effizient mit anderen View-Funktionen zusammenarbeitet.

Bestimmen, ob lokale Benutzerprofile beim Abmelden entfernt werden sollen

Standardmäßig löscht View Persona-Verwaltung die Benutzerprofile nicht von den lokalen Desktops, wenn sich die Benutzer abmelden. Die Richtlinie **[Remove local persona at log off (Lokale Persona beim Abmelden entfernen)]** ist deaktiviert. In vielen Fällen sollte die Standardeinstellung beibehalten werden, da sie die E/A-Vorgänge verringert und redundantes Verhalten vermeidet.

Lassen Sie diese Richtlinie deaktiviert, wenn Sie Pools mit dynamischer Zuweisung bereitstellen und die Desktops beim Abmelden entweder aktualisieren oder löschen. Das lokale Profil wird gelöscht, sobald die virtuelle Maschine aktualisiert oder gelöscht wurde. Bei automatisierten Pools mit dynamischer Zuweisung können vollständige virtuelle Maschinen nach dem Abmelden gelöscht werden. Bei Pools mit dynamischer Zuweisung und verknüpften Klonen können die Klone beim Abmelden aktualisiert oder gelöscht werden.

Wenn Sie Pools mit dedizierter Zuweisung bereitstellen, können Sie die Richtlinie deaktiviert lassen, da die Benutzer bei jeder Sitzung zu denselben Desktops zurückkehren. Wenn die Richtlinie deaktiviert ist und sich ein Benutzer anmeldet, muss View Persona-Verwaltung keine Dateien herunterladen, die im lokalen Profil vorhanden sind. Wenn Sie Pools mit dedizierter Zuweisung und verknüpften Klonen mit persistenten Festplatten konfigurieren, lassen Sie die Richtlinie deaktiviert, um das Löschen von Benutzerdaten von den persistenten Festplatten zu vermeiden.

Unter Umständen möchten Sie die Richtlinie **[Remove local persona at log off (Lokale Persona beim Abmelden entfernen)]** aktivieren.

Umgang mit Bereitstellungen, die View Persona-Verwaltung und servergespeicherte Windows-Profile enthalten

Bei Bereitstellungen, in denen servergespeicherte Windows-Profile konfiguriert werden und Benutzer mit View Persona-Verwaltung und Standard-Desktops mit servergespeicherten Windows-Profilen auf View-Desktops zugreifen, besteht die empfohlene Vorgehensweise darin, verschiedene Profile für die zwei Desktop-Umgebungen zu verwenden. Wenn sich ein View-Desktop und der Clientcomputer, von dem aus der Desktop gestartet wird, innerhalb derselben Domäne befinden und Sie ein Active Directory-GPO zum Konfigurieren sowohl der servergespeicherten Windows-Profile als auch von View Persona-Verwaltung verwenden, aktivieren Sie die Richtlinie **[Persona repository location (Speicherort für das Persona-Repository)]** und wählen Sie **[Override Active Directory user profile path if it is configured (Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist)]** .

Diese Vorgehensweise verhindert, dass servergespeicherte Windows-Profile ein View Persona-Verwaltung-Profil überschreiben, wenn sich der Benutzer vom Clientcomputer abmeldet.

Wenn Benutzer beabsichtigen, Daten zwischen vorhandenen servergespeicherten Windows-Profilen und View Persona-Verwaltung-Profilen auszutauschen, können Sie die Windows-Ordnerumleitung konfigurieren.

Konfiguration von Pfaden für umgeleitete Ordner

Konfigurieren Sie bei Verwendung der Gruppenrichtlinieneinstellung **[Folder redirection (Ordnerumleitung)]** den Ordnerpfad so, dass er den `%Benutzernamen%` enthält, stellen Sie aber gleichzeitig sicher, dass der letzte Unterordner des Pfades den Namen des umgeleiteten Ordners verwendet, so z. B. `Eigene Videos`. Der letzte Ordner im Pfad wird als Ordnername auf dem Desktop des Benutzers angezeigt.

Wenn Sie z. B. einen Pfad wie `\\Eigener Server\Videos\%Benutzername%\Eigene Videos` konfigurieren, wird als Ordnername auf dem Desktop des Benutzers `Eigene Videos` angezeigt.

Ist der `%Benutzername%` der letzte Unterordner im Pfad, wird der Name des Benutzers als Ordnername angezeigt. Der Benutzer `JDoe` sieht dann beispielsweise nicht den Ordner `Eigene Videos` auf dem Desktop, sondern einen Ordner namens `JDoe`, den er nicht problemlos identifizieren kann.

Zusätzliche empfohlene Vorgehensweisen

Sie können auch diese Empfehlungen befolgen:

- Viele Antivirenprodukte scannen standardmäßig Offlinedateien nicht. Wenn ein Benutzer sich z. B. bei einem Desktop anmeldet, scannen solche Antivirenprodukte die Benutzerprofildateien nicht, die nicht in einer der Gruppenrichtlinieneinstellungen **[Files and folders to preload (Dateien und Ordner für das Vorabladen)]** oder **[Windows roaming profiles synchronization (Synchronisierung von servergespeicherten Windows-Profilen)]** angegeben sind. Für viele Bereitstellungen ist das Standardverhalten die empfohlene Vorgehensweise, da sie die E/A verringert, die zum Herunterladen von Dateien bei Scans nach Bedarf anfallen würde.

  Wenn Sie keine Dateien aus dem Remote-Repository abfragen und das Scannen von Offlinedateien aktivieren möchten, lesen Sie die Dokumentation Ihres Antivirenprodukts aufmerksam durch.

- Für die Sicherung von Netzwerkfreigaben, auf denen View Persona-Verwaltung das Profil-Repository speichert, wird die Verwendung von Standard-Vorgehensweisen empfohlen.

  Hinweis Verwenden Sie mit View Persona-Verwaltung keine Sicherungssoftware wie MozyPro oder den Windows Volume-Sicherungsdienst, um Benutzerprofile auf View-Desktops zu sichern.

  View Persona-Verwaltung garantiert, dass Benutzerprofile in das Remote-Profil-Repository gesichert werden, weswegen zur Sicherung von Benutzerdaten auf den Desktops keine zusätzlichen Tools erforderlich sind. In bestimmten Fällen können Tools wie MozyPro oder der Windows Volume-Sicherungsdienst View Persona-Verwaltung beeinträchtigen und einen Datenverlust oder eine Datenbeschädigung hervorrufen.

- Sie können View Persona-Verwaltung-Richtlinien festlegen, um die Leistung zu verbessern, wenn Benutzer ThinApp-Anwendungen starten. Siehe „Konfigurieren von Benutzerprofilen unter Einschluss von ThinApp Sandbox-Ordnern“, auf Seite 222.

- Wenn Ihre Benutzer umfangreiche Persona-Daten generieren und Sie beabsichtigen, zum Verwalten von Desktops mit dedizierter Zuweisung und verknüpften Klonen zu aktualisieren und neu zusammenzustellen, konfigurieren Sie Ihren Desktop-Pool so, dass separate, persistente View Composer-Festplatten verwendet werden. Persistente Festplatten können die Leistung von View Persona-Verwaltung verbessern. Siehe „Konfigurieren von persistenten View Composer-Festplatten mit View Persona-Verwaltung“, auf Seite 223.

Konfigurieren von Benutzerprofilen unter Einschluss von ThinApp Sandbox-Ordnern

View Persona-Verwaltung behält die Benutzereinstellungen bei, die ThinApp-Anwendungen zugewiesen sind, indem ThinApp Sandbox-Ordner in Benutzerprofile eingeschlossen werden. Sie können View Persona-Verwaltung-Richtlinien festlegen, um die Leistung zu verbessern, wenn Benutzer ThinApp-Anwendungen starten.

View Persona-Verwaltung lädt vorab die ThinApp Sandbox-Ordner und -Dateien in das lokale Benutzerprofil, wenn sich ein Benutzer anmeldet. Die ThinApp Sandbox-Ordner werden erstellt, bevor ein Benutzer die Anmeldung abschließen kann. Zwecks Leistungsverbesserung lädt View Persona-Verwaltung die ThinApp Sandbox-Daten beim Anmelden nicht, obwohl sie auf dem lokalen Desktop mit denselben grundlegenden Attributen und Größen wie die ThinApp Sandbox-Dateien im Remote-Profil des Benutzers erstellt werden.

Die empfohlene Vorgehensweise besteht darin, die tatsächlichen ThinApp Sandbox-Daten im Hintergrund herunterzuladen. Aktivieren Sie die Gruppenrichtlinieneinstellung **[Folders to background download (Ordner im Hintergrund herunterladen)]** , und fügen Sie die ThinApp Sandbox-Ordner hinzu. Siehe „Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung“, auf Seite 225.

Die tatsächlichen ThinApp Sandbox-Dateien können groß sein. Bei aktivierter Einstellung **[Folders to background download (Ordner im Hintergrund herunterladen)]** müssen die Benutzer nicht auf das Herunterladen großer Dateien warten, wenn Sie eine Anwendung starten. Außerdem müssen die Benutzer beim Anmelden nicht auf das Vorabladen der Dateien warten. Bei aktivierter Einstellung **[Files and folders to preload (Dateien und Ordner für das Vorabladen)]** wäre das bei großen Dateien der Fall.

Konfigurieren von persistenten View Composer-Festplatten mit View Persona-Verwaltung

Mit persistenten View Composer-Festplatten können Sie Benutzerdaten und Einstellungen speichern, während Sie Betriebssystemfestplatten mit verknüpften Klonen mit den Vorgängen Aktualisieren, Neuzusammenstellung und Neuverteilung verwalten. Das Konfigurieren von persistenten Festplatten kann die Leistung von View Persona-Verwaltung verbessern, wenn die Benutzer große Persona-Datenmengen generieren. Sie können persistente Festplatten nur mit dediziert zugeordneten Desktops mit verknüpften Klonen konfigurieren.

View Persona-Verwaltung speichert jedes Benutzerprofil auf einem Remote-Repository, das auf einer Netzwerkfreigabe konfiguriert ist. Nach der Anmeldung eines Benutzers bei einem Desktop werden die Persona-Dateien dynamisch heruntergeladen, sobald der Benutzer sie benötigt.

Wenn Sie persistente Festplatten mit View Persona-Verwaltung konfigurieren, können Sie die Betriebssystemfestplatten mit verknüpften Klonen aktualisieren und neu zusammenstellen und eine lokale Kopie jedes Benutzerprofils auf den persistenten Festplatten speichern.

Die persistenten Festplatten können als Cache für Benutzerprofile dienen. Wenn ein Benutzer Persona-Dateien benötigt, braucht View Persona-Verwaltung keine Daten herunterzuladen, die identisch auf der lokalen persistenten Festplatte und auf dem Remote-Repository vorliegen. Nur nicht synchronisierte Persona-Daten müssen heruntergeladen werden.

Wenn Sie persistente Festplatten konfigurieren, aktivieren Sie die Richtlinie **[Remove local persona at log off (Lokale Persona beim Abmelden entfernen)]** nicht. Durch das Aktivieren dieser Richtlinie werden die Benutzerdaten beim Abmelden von den persistenten Festplatten gelöscht.

Gruppenrichtlinieneinstellungen für View Persona-Verwaltung

Die View Persona-Verwaltung-ADM-Vorlagendatei enthält Gruppenrichtlinieneinstellungen, die Sie zur Gruppenrichtlinienkonfiguration auf einzelnen Systemen oder einem Active Directory-Server hinzufügen. Sie müssen die Gruppenrichtlinieneinstellungen konfigurieren, um verschiedene Aspekte von View Persona-Verwaltung zu steuern.

Die ADM-Vorlagendatei `ViewPM.adm` ist zusammen mit den anderen View ADM-Vorlagendateien im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware View\Server\extras\GroupPolicyFiles` auf dem View Connection Server-Host installiert.

Wenn Sie View Agent mit der Einrichtungsoption **[View Persona Management (View Persona-Verwaltung)]** installieren, wird die Datei `ViewPM.adm` auch auf der virtuellen Maschine im Verzeichnis *`Installationsverzeichnis`*`\VMware\VMware View\Agent\bin` installiert.

Nachdem Sie die Datei `ViewPM.adm` zu Ihrer Gruppenrichtlinienkonfiguration hinzugefügt haben, befinden sich die Richtlinieneinstellungen im Ordner **[Persona-Verwaltung]** im Gruppenrichtlinienfenster.

Tabelle 9-1. Speicherort der View Persona-Verwaltung-Einstellungen im Gruppenrichtlinienfenster

Betriebssystem	Standort
Windows Vista und höher oder Windows Server 2008 und höher	**[Computer Configuration (Computerkonfiguration)] > [Administrative Templates (Administrative Vorlagen)] > [Classic Administrative Templates (Administrative Vorlagen)] > [VMware VMware View Agent Configuration (View Agent-Konfiguration)] > [Persona-Verwaltung]**
Windows XP oder Windows Server 2003	**[Computer Configuration (Computerkonfiguration)] > [Administrative Templates (Administrative Vorlagen)] > [VMware View Agent Configuration (VMware View Agent-Konfiguration)] > [Persona-Verwaltung]**

Die Gruppenrichtlinieneinstellungen befinden sich in diesen Ordnern:

- Roaming (Serverspeicherung) & Synchronization (Synchronisierung)
- Ordnerumleitung
- Desktop-Benutzeroberfläche
- Logging (Protokollieren)

Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung

Die Gruppenrichtlinieneinstellungen für Serverspeicherung und Synchronisierung schalten View Persona-Verwaltung ein und aus, legen den Speicherort des Remote-Profil-Repositorys fest, bestimmen, welche Ordner und Dateien zum Benutzerprofil gehören, und steuern, wie Dateien und Ordner synchronisiert werden.

Gruppenrichtlinieneinstellung	Beschreibung
Manage user persona (Benutzerpersona verwalten)	Bestimmt, ob Benutzerprofile dynamisch mit View Persona-Verwaltung oder mit servergespeicherten Windows-Profilen verwaltet werden sollen. Diese Einstellung schaltet View Persona-Verwaltung ein und aus. Wenn diese Einstellung aktiviert ist, verwaltet View Persona-Verwaltung die Benutzerprofile. Wenn diese Einstellung aktiviert ist, können Sie ein Profiluploadintervall in Minuten angeben. Dieser Wert bestimmt, wie oft Änderungen am Benutzerprofil in das Remote-Repository kopiert werden. Der Standardwert lautet 10 Minuten. Wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde, werden die Benutzerprofile von Windows verwaltet.
Persona repository location (Speicherort für das Persona-Repository)	Gibt den Speicherort des Benutzerprofil-Repositorys an. Diese Einstellung bestimmt auch, ob eine in View Persona-Verwaltung angegebene Netzwerkfreigabe oder ein in Active Directory konfigurierter Pfad verwendet wird, um servergespeicherte Windows-Profile zu unterstützen. Wenn diese Einstellung aktiviert ist, können Sie **[Share path (Freigabepfad)]** verwenden, um den Speicherort des Benutzerprofil-Repositorys zu bestimmen. Im Textfeld **[Share path (Freigabepfad)]** geben Sie einen UNC-Pfad zu einer Netzwerkfreigabe an, auf die View Persona-Verwaltungs-Desktops zugreifen können. Mit dieser Einstellung kann View Persona-Verwaltung den Speicherort des Benutzerprofil-Repositorys steuern. Beispiel: `\\server.domain.com\VPRepository` Wenn `%Benutzername%` nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona-Verwaltung `%Benutzername%.%Benutzerdomäne%` an den Pfad an. Beispiel: `\\server.domain.com\VPRepository\%Benutzername%.%Benutzerdomäne%` Wenn Sie unter **[Share path (Freigabepfad)]** einen Speicherort angeben, müssen Sie weder in Windows servergespeicherte Profile einrichten noch einen Benutzerprofilpfad in Active Directory konfigurieren, um servergespeicherte Windows-Profile zu unterstützen. Detaillierte Informationen zum Konfigurieren einer UNC-Netzwerkfreigabe für View Persona-Verwaltung finden Sie unter „Konfigurieren eines Benutzerprofil-Repositorys“, auf Seite 213. Standardmäßig wird der Active Directory-Benutzerprofilpfad verwendet. Wenn **[Share path (Freigabepfad)]** leer gelassen wurde, wird der Active Directory-Benutzerprofilpfad verwendet. Der **[Share path (Freigabepfad)]** ist leer und inaktiv, wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde. Sie können den Pfad auch leer lassen, wenn diese Einstellung aktiviert wurde. Wenn diese Einstellung aktiviert wurde, können Sie das Kontrollkästchen **[Override Active Directory user profile path if it is configured (Active Directory-Benutzerprofilpfad außer Kraft setzen, wenn er konfiguriert ist)]** markieren, um sicherzustellen, dass View Persona-Verwaltung den in **[Share path (Freigabepfad)]** angegebenen Pfad verwendet. Standardmäßig ist dieses Kontrollkästchen nicht markiert, und View Persona-Verwaltung verwendet den Active Directory-Benutzerprofilpfad, wenn beide Speicherorte konfiguriert sind.
Remove local persona at log off (Lokale Persona beim Abmelden entfernen)	Löscht das lokal gespeicherte Profil jedes Benutzers aus dem Desktop-System, wenn sich der Benutzer abmeldet. Sie können auch ein Kästchen markieren, um die Ordner mit den lokalen Einstellungen jedes Ordners zu löschen, wenn das Benutzerprofil entfernt wird. Unter Windows 7 und Windows Vista führt das Markieren dieses Kästchens zum Löschen des Ordners `AppData\Local`. In Windows XP führt das Markieren dieses Kästchens zum Löschen des Ordners `Local Settings`. Anweisungen zum Verwenden dieser Einstellungen finden Sie unter „Empfohlene Vorgehensweisen beim Konfigurieren einer View Persona-Verwaltung-Bereitstellung“, auf Seite 220. Wenn diese Einstellung deaktiviert oder nicht konfiguriert wurde, werden die lokal gespeicherten Benutzerprofile, einschließlich der Ordner mit den lokalen Einstellungen, beim Abmelden des Benutzers nicht gelöscht.

Gruppenrichtlinieneinstellung	Beschreibung
Roam local settings folders (Ordner mit den lokalen Einstellungen auf dem Server speichern)	Speichert die Ordner mit den lokalen Einstellungen mit dem Rest jedes Benutzerprofils auf dem Server. Bei Windows 7 oder Windows Vista betrifft diese Richtlinie den Ordner `AppData\Local`. Bei Windows XP betrifft diese Richtlinie den Ordner `Local Settings`. Standardmäßig werden die lokalen Einstellungen nicht auf dem Server gespeichert.
Files and folders to preload (Dateien und Ordner für das Vorabladen)	Gibt eine Liste mit Dateien und Ordnern an, die in das lokale Benutzerprofil heruntergeladen werden, wenn sich der Benutzer anmeldet. Änderungen an den Dateien werden in das Remote-Repository kopiert, sobald sie auftreten. In einigen Situationen möchten Sie möglicherweise bestimmte Dateien und Ordner vorab in das lokal gespeicherte Benutzerprofil laden. Verwenden Sie diese Einstellung, um diese Dateien und Ordner anzugeben. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an. Beispiel: `Anwendungsdaten\Microsoft\Certificates` Nachdem die angegebenen Dateien und Ordner vorab geladen wurden, verwaltet View Persona-Verwaltung die Dateien und Ordner auf dieselbe Weise wie andere Profildaten. Wenn ein Benutzer vorab geladene Dateien oder Ordner ändert, kopiert View Persona-Verwaltung die aktualisierten Daten während der Sitzung im darauffolgenden Profiluploadintervall in das Remote-Profil-Repository.
Files and folders to preload (exceptions) (Dateien und Ordner für das Vorabladen (Ausnahmen))	Verhindert, dass die angegebenen Dateien und Ordner vorab geladen werden. Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung **[Files and folders to preload (Dateien und Ordner für das Vorabladen)]** angegeben haben. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.
Windows roaming profiles synchronization (Synchronisierung von servergespeicherten Windows-Profilen)	Gibt eine Liste mit Dateien und Ordnern an, die von standardmäßigen servergespeicherten Windows-Profilen verwaltet werden. Die Dateien und Ordner werden vom Remote-Repository abgerufen, wenn sich der Benutzer anmeldet. Die Dateien werden erst in das Remote-Repository kopiert, wenn sich der Benutzer abmeldet. Für die angegebenen Dateien und Ordner ignoriert View Persona-Verwaltung das Profilreplikationsintervall, das durch **[Profile upload interval (Profilhochladeintervall)]** in der Einstellung **[Manage user persona (Benutzerpersona verwalten)]** konfiguriert ist. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.
Windows roaming profiles synchronization (exceptions) (Synchronisierung von servergespeicherten Windows-Profilen (Ausnahmen))	Die ausgewählten Dateien und Ordner sind Ausnahmen der Pfade, die in der Einstellung **[Windows roaming profiles synchronization (Synchronisierung von servergespeicherten Windows-Profilen)]** angegeben sind. Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung **[Windows roaming profiles synchronization (Synchronisierung von servergespeicherten Windows-Profilen)]** angegeben haben. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.
Files and folders excluded from roaming (Von der Serverspeicherung ausgenommene Dateien und Ordner)	Gibt eine Liste der Ordner und Dateien an, die nicht mit dem Rest des Benutzerprofils auf dem Server gespeichert werden. Die angegebenen Dateien und Ordner sind nur auf dem lokalen System vorhanden. In manchen Situationen ist es erforderlich, dass bestimmte Dateien und Ordner nur im lokal gespeicherten Benutzerverzeichnis vorhanden sind. Sie können beispielsweise temporäre Dateien und zwischengespeicherte Dateien vom Roaming ausschließen. Diese Dateien müssen nicht in das Remote-Repository repliziert werden. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an. Standardmäßig sind die folgenden Ordner ausgenommen: der temporäre Ordner des Benutzerprofils, der Ordner des ThinApp-Caches und die Cache-Ordner für Internet Explorer, Firefox, Chrome und Opera.

Gruppenrichtlinieneinstellung	Beschreibung
Files and folders excluded from roaming (exceptions) (Von der Serverspeicherung ausgenommene Dateien und Ordner (Ausnahmen))	Die ausgewählten Dateien und Ordner sind Ausnahmen von den Pfaden, die in der Einstellung **[Files and folders excluded from roaming (Von der Serverspeicherung ausgenommene Dateien und Ordner)]** angegeben sind. Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung **[Files and folders excluded from roaming (Von der Serverspeicherung ausgenommene Dateien und Ordner)]** angegeben haben. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.
Folders to background download (Im Hintergrund herunterzuladende Ordner)	Die ausgewählten Ordner werden nach der Anmeldung des Benutzers beim Desktop im Hintergrund heruntergeladen. In bestimmten Fällen können Sie View Persona-Verwaltung optimieren, indem Sie den Inhalt bestimmter Ordner im Hintergrund herunterladen. Bei aktivierter Einstellung müssen die Benutzer nicht auf das Herunterladen großer Dateien warten, wenn sie eine Anwendung starten. Außerdem müssen die Benutzer beim Anmelden nicht auf das Vorabladen der Dateien warten. Bei aktivierter Einstellung **[Files and folders to preload (Dateien und Ordner für das Vorabladen)]** wäre das bei sehr großen Dateien der Fall. Sie können z. B. VMware ThinApp Sandbox-Ordner in der Einstellung **[Folders to background download (Im Hintergrund herunterzuladende Ordner)]** einbeziehen. Das Herunterladen im Hintergrund beeinträchtigt die Leistung nicht, wenn sich ein Benutzer anmeldet oder andere Anwendungen auf dem Desktop verwendet. Wenn der Benutzer die ThinApp-Anwendung startet, werden die erforderlichen ThinApp Sandbox-Dateien wahrscheinlich vom Remote-Repository heruntergeladen und verkürzen so die Startzeit der Anwendung. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.
Folders to background download (exceptions) (Im Hintergrund herunterzuladende Ordner) (Ausnahmen))	Die ausgewählten Ordner sind Ausnahmen von den Pfaden, die in der Einstellung **[Folders to background download (Im Hintergrund herunterzuladende Ordner)]** festgelegt sind. Die ausgewählten Ordnerpfade müssen sich in den Ordnern befinden, die Sie in der Einstellung **[Folders to background download (Im Hintergrund herunterzuladende Ordner)]** angegeben haben. Geben Sie Pfade relativ zum Stamm des lokalen Profils an. Geben Sie in einem Pfadnamen kein Laufwerk an.

Gruppenrichtlinieneinstellungen für Ordnerumleitung

Mit Gruppenrichtlinieneinstellungen für Ordnerumleitung können Sie Benutzerprofilordner auf eine Netzwerkfreigabe umleiten. Wenn ein Ordner umgeleitet wird, werden alle Daten während der Benutzersitzung direkt auf der Netzwerkfreigabe gespeichert.

Sie können diese Einstellungen verwenden, um Ordner umzuleiten, die hochgradig verfügbar sein müssen. View Persona-Verwaltung kopiert die Aktualisierungen vom lokalen Benutzerprofil häufig in das Remote-Profil, bis zu einmal pro Minute, abhängig vom Wert, den Sie für das Profiluploadintervall festgelegt haben. Wenn es auf dem lokalen System jedoch zu einem Netzwerkausfall oder -fehler kommt, werden die Aktualisierungen eines Benutzers seit der letzten Replikation möglicherweise nicht in das Remote-Profil gespeichert. In Situationen, bei denen es für die Benutzer ausgeschlossen ist, einen temporären Datenverlust der Arbeit der letzten paar Minuten hinzunehmen, können Sie jene Ordner umleiten, in denen diese kritischen Daten gespeichert werden.

Die folgenden Regeln und Richtlinien gelten für die Ordnerumleitung:

- Wenn Sie diese Einstellung für einen Ordner aktivieren, müssen Sie den UNC-Pfad der Netzwerkfreigabe eingeben, auf die der Ordner umgeleitet wird.
- Wenn `%Benutzername%` nicht im von Ihnen konfigurierten Ordnerpfad enthalten ist, hängt View Persona-Verwaltung `%Benutzername%` an den UNC-Pfad an.

- Konfigurieren Sie als empfohlene Vorgehensweise den Ordnerpfad so, dass er den `%Benutzernamen%` enthält, stellen Sie aber gleichzeitig sicher, dass der letzte Unterordner des Pfades den Namen des umgeleiteten Ordners verwendet, so z. B. `Eigene Videos`. Der letzte Ordner im Pfad wird als Ordnername auf dem Desktop des Benutzers angezeigt. Weitere Informationen finden Sie unter „Konfiguration von Pfaden für umgeleitete Ordner“, auf Seite 221.
- Sie können für jeden Ordner separate Einstellungen konfigurieren. Sie können bestimmte Ordner für die Umleitung auswählen und andere auf dem lokalen View-Desktop belassen. Sie können auch verschiedene Ordner auf verschiedene UNC-Pfade umleiten.
- Wenn eine Ordnerumleitungseinstellung deaktiviert oder nicht konfiguriert wurde, wird der Ordner auf dem lokalen View-Desktop gespeichert und gemäß den View Persona-Verwaltung-Gruppenrichtlinieneinstellungen verwaltet.
- Wenn View Persona-Verwaltung und servergespeicherte Windows-Profile zur Umleitung desselben Ordners konfiguriert wurden, hat die View Persona-Verwaltung-Ordnerumleitung Vorrang vor servergespeicherten Windows-Profilen.
- Die Ordnerumleitung gilt für alle Anwendungen, die die Windows Shell-APIs verwenden, um gemeinsame Ordnerpfade umzuleiten. Wenn beispielsweise eine Anwendung eine Datei in `%Benutzerprofil%\AppData\Roaming` schreibt, wird die Datei in das lokale Profil geschrieben und nicht an einen Netzwerkspeicherort umgeleitet.

Sie können die folgenden Ordner auf eine Netzwerkfreigabe umleiten:

- Anwendungsdaten (servergespeichert)
- Kontakte
- Cookies
- Desktop
- Downloads
- Favoriten
- Verlauf
- Links
- Eigene Dateien
- Eigene Musik
- Eigene Bilder
- Eigene Videos
- Netzwerkumgebung
- Druckerumgebung
- Zuletzt verwendet
- Gespeicherte Spiele
- Suchvorgänge
- Startmenü
- Startobjekte
- Vorlagen
- Temporäre Internetdateien

Bestimmte Ordner sind nur unter Windows Vista und neueren Betriebssystemen verfügbar.

Gruppenrichtlinieneinstellungen für Desktop-Benutzeroberfläche

Die Gruppenrichtlinieneinstellungen für Desktop-Benutzeroberfläche steuern die View Persona-Verwaltung-Einstellungen, die die Benutzer auf ihren Desktops sehen.

Gruppenrichtlinieneinstellung	Beschreibung
Hide local offline file icon (Lokales Offline-Dateisymbol ausblenden)	Bestimmt, ob das Offline-Symbol ausgeblendet wird, wenn ein Benutzer lokal gespeicherte Dateien anzeigt, die zum Benutzerprofil gehören. Durch Aktivieren dieser Einstellung wird das Offline-Symbol in Windows Explorer und in den meisten Windows-Dialogfeldern ausgeblendet. Das Offline-Symbol ist standardmäßig ausgeblendet.
Show progress when downloading large files (Beim Herunterladen von großen Dateien Fortschritt anzeigen)	Legt fest, ob beim Herunterladen von Dateien ein Fortschrittsfenster auf dem Benutzer-Desktop angezeigt wird, wenn der Client große Dateien aus dem Remote-Repository abruft. Bei Aktivierung dieser Einstellung können Sie die Mindestdateigröße (in Megabyte) angeben, ab der beim Herunterladen von Dateien ein Fortschrittsfenster angezeigt wird. Das Fenster wird angezeigt, wenn View Persona-Verwaltung bestimmt, dass die angegebene Datenmenge vom Remote-Repository abgerufen wird. Dieser Wert ist die Summe für alle Dateien, die in einem Arbeitsschritt abgerufen werden. Wenn z. B. der Einstellungswert 50 MB lautet und eine 40 MB große Datei abgerufen wird, wird dieses Fenster nicht angezeigt. Wenn eine 30 MB große Datei abgerufen wird, während die erste Datei noch heruntergeladen wird, überschreitet die Summe beider Dateien den Wert und das Fortschrittsfenster wird angezeigt. Das Fenster wird beim Start des Downloadvorgangs einer Datei angezeigt. Dieser Wert ist standardmäßig auf 50 MB festgelegt. Das Fortschrittsfenster wird standardmäßig nicht angezeigt.
Show critical errors to users via tray icon alerts (Benutzern kritische Fehler über Leistensymbolwarnungen anzeigen)	Zeigt Benutzern kritische Fehler über Symbole in der Desktop-Leiste an, wenn es bei der Replikation oder bei der Netzwerkkonnektivität zu Fehlern kommt. Diese Symbolwarnungen sind standardmäßig ausgeblendet.

Protokollieren von Gruppenrichtlinieneinstellungen

Die Gruppenrichtlinieneinstellungen zum Protokollieren bestimmen den Namen, den Speicherort und das Verhalten von Persona-Verwaltung-Protokolldateien.

Gruppenrichtlinieneinstellung	Beschreibung
Logging filename (Name der Protokolldatei)	Gibt den vollständigen Pfadnamen der lokalen Protokolldatei von View Persona-Verwaltung an. Auf Windows 7-Computern lautet der Standardpfad `Programme\VMware\VDM\logs\`*`Dateiname`*. Auf Windows XP-Computern lautet der Standardpfad *`All Users`*`\Anwendungsdaten\VMware\VDM\logs\`*`Dateiname`*. Der standardmäßige Protokolldateiname ist `VMWVvp.txt`.
Logging destination (Protokollierungsziel)	Legt fest, ob alle Protokollmeldungen in die Protokolldatei, den Debug-Bericht oder in beide Ziele geschrieben werden. Standardmäßig werden Protokollmeldungen in der Protokolldatei ausgegeben.

Gruppenrichtlinieneinstellung	Beschreibung
Logging flags (Protokollierungskennzeichen)	Legt die Art der zu protokollierenden Meldungen fest. Wenn diese Einstellung konfiguriert ist, können Sie einige oder alle der folgenden Protokollmeldungstypen generieren: ■ Fehlermeldungen protokollieren ■ Informationsmeldungen protokollieren ■ Debug-Meldungen protokollieren Standardmäßig werden Fehler- und Informations-Protokollmeldungstypen generiert.
Debug flags (Debug-Kennzeichen)	Legt die Art der zu protokollierenden Debug-Meldungen fest. View Persona Management verarbeitet Debugmeldungen auf dieselbe Weise wie Protokollmeldungen. Wenn diese Einstellung aktiviert ist, können Sie einige oder alle der folgenden Debugmeldungstypen auswählen: ■ Debugfehlermeldungen ■ Debuginformationsmeldungen ■ Debug-Registry-Meldungen ■ Debug-IRQ-Meldungen ■ Debug-Port-Meldungen ■ Debugverarbeitungsmeldungen Standardmäßig werden keine Debug-Meldungen generiert.

Verwalten von Linked-Clone-Desktops 10

Mit View Composer können Sie Linked-Clone-Desktops aktualisieren, die Größe der Betriebssystemdaten reduzieren und eine Neuverteilung der virtuellen Linked-Clone-Maschinen auf die Festplattenlaufwerke vornehmen. Darüber hinaus können Sie die persistenten View Composer-Festplatten von verknüpften Klonen verwalten.

- Reduzieren der Größe von verknüpften Klonen durch eine Desktop-Aktualisierung auf Seite 231

  Bei einer Desktop-Aktualisierung werden der ursprüngliche Status und die ursprüngliche Größe der Betriebssystemfestplatten der einzelnen verknüpften Klone wiederhergestellt und damit die Speicherkosten reduziert.

- Aktualisieren von Linked-Clone-Desktops auf Seite 233

  Linked-Clone-Desktops können aktualisiert werden, indem Sie ein neues Basis-Image für die übergeordnete virtuelle Maschine erstellen und das aktualisierte Image mithilfe der Neuzusammenstellungsfunktion an die verknüpften Klone verteilen.

- Neuverteilen von Linked-Clone-Desktops auf Seite 238

  Bei einem Vorgang zur Neuverteilung für einen Desktop werden Linked-Clone-Desktops erneut auf die verfügbaren Datenspeicher verteilt.

- Verwalten persistenter View Composer-Festplatten auf Seite 241

  Sie können eine persistente Festplatte von einem Linked-Clone-Desktop trennen und mit einem anderen verknüpften Klon verknüpfen. Mithilfe dieser Funktion können Sie Benutzerinformationen getrennt von den Linked-Clone-Desktops verwalten.

Reduzieren der Größe von verknüpften Klonen durch eine Desktop-Aktualisierung

Bei einer Desktop-Aktualisierung werden der ursprüngliche Status und die ursprüngliche Größe der Betriebssystemfestplatten der einzelnen verknüpften Klone wiederhergestellt und damit die Speicherkosten reduziert.

Planen Sie Aktualisierungsvorgänge wenn möglich außerhalb der Spitzenzeiten.

Richtlinien finden Sie unter „Desktop-Aktualisierungen“, auf Seite 232.

Voraussetzungen

- Legen Sie den Zeitpunkt für die Aktualisierung fest. Standardmäßig startet View Composer den Vorgang sofort.

  Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Aktualisierung planen. Sie können mehrere Vorgänge zur Aktualisierung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald der Vorgang gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor der Desktop des jeweiligen Benutzers aktualisiert wird.

  Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View Manager, sodass sie ihre Anwendungen schließen und sich abmelden können.

- Wenn Ihre Bereitstellung replizierte View Connection Server-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Doppelklicken Sie zur Auswahl des Pools für die Aktualisierung in der linken Spalte auf die Pool-ID.

3 Legen Sie fest, ob der gesamte Pool oder nur ausgewählte Desktops aktualisiert werden sollen.

Option	Aktion
To refresh all desktops in the pool (Aktualisierung aller Desktops im Pool)	Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Settings (Einstellungen)]** .
To refresh selected desktops (Aktualisierung ausgewählter Desktops)	a Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Inventory (Bestandsliste)]** . b Wählen Sie die zu aktualisierenden Desktops.

4 Klicken Sie auf **[View Composer] > [Aktualisierung]** .

5 Befolgen Sie die Anweisungen des Assistenten, um die Linked-Clone-Desktops zu aktualisieren.

Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

Der Fortschritt des Aktualisierungsvorgangs für die virtuellen Linked-Clone-Maschinen kann in vCenter Server überwacht werden.

In View Administrator können Sie den Vorgang überwachen, indem Sie auf **[Inventory (Bestandsliste)] > [Pools]** klicken, die Pool-ID auswählen und anschließend auf die Registerkarte **[Tasks (Aufgaben)]** klicken. Zum Beenden, Anhalten oder Fortsetzen einer angehaltenen Aufgabe klicken Sie auf **[Cancel Task (Aufgabe abbrechen)]** , **[Pause Task (Aufgabe anhalten)]** oder **[Resume Task (Aufgabe fortsetzen)]** .

Desktop-Aktualisierungen

Wenn Benutzer mit Linked-Clone-Desktops interagieren, steigt die Größe der Betriebssystemfestplatte der Klone. Bei einer Desktop-Aktualisierung werden der ursprüngliche Status und die ursprüngliche Größe der Betriebssystemfestplatte wiederhergestellt und damit die Speicherkosten reduziert.

Eine Aktualisierung hat keine Auswirkungen auf persistente View Composer-Festplatten.

Ein verknüpfter Klon verwendet weniger Speicherplatz als die übergeordnete virtuelle Maschine, welche die gesamten Betriebssystemdaten umfasst. Die Betriebssystemfestplatte eines Klons wird jedoch bei jedem Schreibvorgang für Daten aus dem Betriebssystem vergrößert.

Beim Erstellen eines verknüpften Klons durch View Composer wird ein Snapshot der Betriebssystemfestplatte des Klons erstellt. Der Snapshot kennzeichnet die virtuelle Linked-Clone-Maschine eindeutig. Bei einer Aktualisierung wird die Betriebssystemfestplatte anhand des Snapshots wiederhergestellt.

View Composer kann einen verknüpften Klon in der Hälfte der Zeit aktualisieren, die für das Löschen und erneute Erstellen des Klons benötigt wird.

Befolgen Sie bei Aktualisierungen die folgenden Richtlinien:

- Sie können einen Desktop-Pool nach Bedarf, als geplantes Ereignis oder beim Erreichen einer festgelegten Größe der Betriebssystemfestplatte aktualisieren.

Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Aktualisierung planen. Wenn Sie eine Aktualisierung umgehend starten, setzt der Vorgang zuvor geplante Aufgaben außer Kraft.

Sie können mehrere Vorgänge zur Aktualisierung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

Bevor Sie einen Vorgang zur Aktualisierung planen, müssen Sie zuvor geplante Aufgaben abbrechen.

- Sie können Pools mit dedizierter und mit dynamischer Zuweisung aktualisieren.
- Sie können keine Desktops aktualisieren, die lokale Sitzungen ausführen.
- Eine Aktualisierung kann nur ausgeführt werden, wenn die Benutzer von ihren View-Desktops getrennt sind.
- Bei der Aktualisierung werden die über QuickPrep oder Sysprep eingerichteten eindeutigen Computerinformationen beibehalten. Sysprep muss nach einer Aktualisierung nicht erneut ausgeführt werden, um die SID oder die GUIDs von auf dem Systemlaufwerk installierter Drittanbietersoftware wiederherzustellen.
- Nach der Neuzusammenstellung eines verknüpften Klons erstellt View Manager einen neuen Snapshot der Betriebssystemfestplatte des verknüpften Klons. Bei zukünftigen Aktualisierungen werden die Betriebssystemdaten basierend auf diesem Snapshot wiederhergestellt, nicht anhand des Snapshots, der bei der ursprünglichen Erstellung des verknüpften Klons erstellt wurde.

Hinweis Sie können das Wachstum verknüpfter Klone verlangsamen, indem Sie die Auslagerungsdateien und temporären Systemdateien auf eine temporäre Festplatte umleiten. Beim Ausschalten eines verknüpften Klons ersetzt View Manager die temporäre Festplatte durch eine Kopie der ursprünglichen temporären Festplatte, die View Composer mit dem Linked-Clone-Pool erstellt hat. Bei diesem Vorgang wird die temporäre Festplatte auf die ursprüngliche Größe reduziert.

Sie können diese Option beim Erstellen eines Linked-Clone-Pools konfigurieren.

Aktualisieren von Linked-Clone-Desktops

Linked-Clone-Desktops können aktualisiert werden, indem Sie ein neues Basis-Image für die übergeordnete virtuelle Maschine erstellen und das aktualisierte Image mithilfe der Neuzusammenstellungsfunktion an die verknüpften Klone verteilen.

- Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von Linked-Clone-Desktops auf Seite 234

  Bevor Sie einen Linked-Clone-Desktop-Pool neu zusammenstellen, muss die übergeordnete virtuelle Maschine aktualisiert werden, die als Basis-Image für die verknüpften Klone verwendet wurde.

- Neuzusammenstellung von Linked-Clone-Desktops auf Seite 234

  Bei der Desktop-Neuzusammenstellung werden alle mit einer übergeordneten virtuellen Maschine verknüpften Linked-Clone-Desktops gleichzeitig aktualisiert.

- Neuzusammenstellung von Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden können auf Seite 236

  Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden können, können neu zusammengestellt werden. Die Desktops müssen jedoch eingecheckt werden, oder Sie müssen für diese Desktops ein Rollback durchführen, um den Vorgang zur Neuzusammenstellung ausführen zu können.

- Aktualisieren verknüpfter Klone bei der Desktop-Neuzusammenstellung auf Seite 237

  Bei einer Desktop-Neuzusammenstellung können Sie Betriebssystem-Patches bereitstellen, Anwendungen installieren bzw. aktualisieren oder die Desktop-Hardwareeinstellungen aller verknüpften Klone in einem Desktop-Pool ändern.

- Korrigieren einer nicht erfolgreichen Neuzusammenstellung auf Seite 238

  Eine fehlgeschlagene Neuzusammenstellung kann korrigiert werden. Sie können zudem korrigierende Maßnahmen ergreifen, wenn Sie verknüpfte Klone versehentlich unter Verwendung eines falschen Basis-Images neu zusammenstellen.

Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von Linked-Clone-Desktops

Bevor Sie einen Linked-Clone-Desktop-Pool neu zusammenstellen, muss die übergeordnete virtuelle Maschine aktualisiert werden, die als Basis-Image für die verknüpften Klone verwendet wurde.

View Composer bietet keine Unterstützung für die Neuzusammenstellung verknüpfter Klone in einer übergeordneten virtuellen Maschine, wenn der verknüpfte Klon ein anderes Betriebssystem verwendet als die übergeordnete virtuelle Maschine. Beispielsweise kann ein Snapshot einer übergeordneten virtuellen Maschine mit Windows 7 oder Windows Vista nicht verwendet werden, um einen verknüpften Klon mit Windows XP neu zusammenzustellen.

Vorgehensweise

1 Aktualisieren Sie die übergeordnete virtuelle Maschine in vCenter Server für die Neuzusammenstellung.

   - Installieren Sie Betriebssystem-Patches oder Service Packs, neue Anwendungen, Anwendungs-Updates oder nehmen Sie andere Änderungen an der übergeordneten virtuellen Maschine vor.
   - Alternativ bereiten Sie eine andere virtuelle Maschine vor, die bei der Neuzusammenstellung als neue übergeordnete virtuelle Maschine verwendet werden soll.

2 Schalten Sie die aktualisierte oder neue übergeordnete virtuelle Maschine in vCenter Server aus.

3 Erstellen Sie in vCenter Server einen Snapshot der übergeordneten virtuellen Maschine.

Weiter

Stellen Sie den Linked-Clone-Desktop-Pool neu zusammen.

Neuzusammenstellung von Linked-Clone-Desktops

Bei der Desktop-Neuzusammenstellung werden alle mit einer übergeordneten virtuellen Maschine verknüpften Linked-Clone-Desktops gleichzeitig aktualisiert.

Planen Sie Neuzusammenstellungen wenn möglich außerhalb der Spitzenzeiten.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Snapshot der übergeordneten virtuellen Maschine verfügen. Siehe „Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von Linked-Clone-Desktops“, auf Seite 234.
- Machen Sie sich mit den Richtlinien zur Neuzusammenstellung vertraut. Siehe „Aktualisieren verknüpfter Klone bei der Desktop-Neuzusammenstellung“, auf Seite 237.
- Legen Sie den Zeitpunkt für die Neuzusammenstellung fest. Standardmäßig startet View Composer die Neuzusammenstellung sofort.

  Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur eine Neuzusammenstellung planen. Sie können mehrere Neuzusammenstellungen planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald die Neuzusammenstellung gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor für den Desktop des jeweiligen Benutzers eine Neuzusammenstellung vorgenommen wird.

  Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View Manager, sodass sie ihre Anwendungen schließen und sich abmelden können.

- Legen Sie fest, ob Sie die Bereitstellung beim ersten Fehler abbrechen möchten. Wenn Sie diese Option auswählen und bei der Bereitstellung eines verknüpften Klons durch View Composer ein Fehler auftritt, wird die Bereitstellung für alle Klone im Pool abgebrochen. Sie können diese Option auswählen, um sicherzustellen, dass die Ressourcen wie Speicher nicht unnötigerweise beansprucht werden.

  Die Auswahl der Option **[Stop at first error (Beim ersten Fehler abbrechen)]** hat keinen Einfluss auf die Anpassung. Tritt ein Anpassungsfehler bei einem verknüpften Klon auf, wird die Bereitstellung und Anpassung für die anderen Klone weiter fortgeführt.

- Stellen Sie sicher, dass die Bereitstellung für den Pool aktiviert ist. Wenn die Bereitstellung für den Pool deaktiviert ist, verhindert View Manager eine Anpassung der Desktops nach deren Neuzusammenstellung.

- Wenn Ihre Bereitstellung replizierte View Connection Server-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Doppelklicken Sie zur Auswahl des Pools für die Neuzusammenstellung in der linken Spalte auf die Pool-ID.

3 Legen Sie fest, ob der gesamte Pool oder nur ausgewählte Desktops neu zusammengestellt werden sollen.

Option	Aufgabe
To recompose all desktops in the pool (Neuzusammenstellung aller Desktops im Pool)	Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Settings (Einstellungen)]** .
To recompose selected desktops (Neuzusammenstellung ausgewählter Desktops)	a Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Inventory (Bestandsliste)]** . b Wählen Sie die Desktops, für die eine Neuzusammenstellung vorgenommen werden soll.

4 Klicken Sie auf **[View Composer] > [Neuzusammenstellung]** .

5 Befolgen Sie die Anweisungen des Assistenten, um für die Linked-Clone-Desktops eine Neuzusammenstellung vorzunehmen.

  Wenn Sie den gesamten Pool über die Registerkarte **[Settings (Einstellungen)]** neu zusammenstellen, können Sie das Kontrollkästchen **[Change the default image for new desktops (Standard-Image für neue Desktops ändern)]** aktivieren. Mit dieser Einstellung verwenden neue Desktops, die im Pool erstellt werden, das aktualisierte Basis-Image. Diese Einstellung ist standardmäßig aktiviert.

  Auf der Seite **[Ready to Complete (Bereit zum Abschließen)]** können Sie auf **[Show Details (Details anzeigen)]** klicken, um die Linked-Clone-Desktops anzuzeigen, die neu zusammengestellt werden.

Die Linked-Clone-Desktops werden aktualisiert. Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

In einem Pool mit dedizierter Zuweisung werden verknüpfte Klone ohne Zuweisung gelöscht und neu erstellt. Die angegebene Anzahl an Reserve-Desktops wird beibehalten.

In einem Pool mit dynamischer Zuweisung werden alle ausgewählten verknüpften Klone neu zusammengestellt.

Der Fortschritt der Neuzusammenstellung für die virtuellen Linked-Clone-Maschinen kann in vCenter Server überwacht werden.

In View Administrator können Sie den Vorgang überwachen, indem Sie auf **[Inventory (Bestandsliste)] > [Pools]** klicken, die Pool-ID auswählen und anschließend auf die Registerkarte **[Tasks (Aufgaben)]** klicken. Zum Beenden, Anhalten oder Fortsetzen einer angehaltenen Aufgabe klicken Sie auf **[Cancel Task (Aufgabe abbrechen)]** , **[Pause Task (Aufgabe anhalten)]** oder **[Resume Task (Aufgabe fortsetzen)]** .

Hinweis Wenn Sie bei der Erstellung des Desktop-Pools zur Anpassung der verknüpften Klone eine Sysprep-Anpassungsspezifikation verwendet haben, werden für die neu zusammengestellten virtuellen Maschinen möglicherweise neue SIDs generiert. Weitere Informationen finden Sie unter „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“, auf Seite 102.

Neuzusammenstellung von Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden können

Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden können, können neu zusammengestellt werden. Die Desktops müssen jedoch eingecheckt werden, oder Sie müssen für diese Desktops ein Rollback durchführen, um den Vorgang zur Neuzusammenstellung ausführen zu können.

Voraussetzungen

- Machen Sie sich mit den Richtlinien zur Neuzusammenstellung vertraut. Siehe „Aktualisieren verknüpfter Klone bei der Desktop-Neuzusammenstellung“, auf Seite 237.
- Machen Sie sich mit der Vorgehensweise zur Aktualisierung des Basis-Images und zur Neuzusammenstellung von Linked-Clone-Desktops vertraut. Siehe „Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung von Linked-Clone-Desktops“, auf Seite 234 und „Neuzusammenstellung von Linked-Clone-Desktops“, auf Seite 234.
- Machen Sie sich mit der Vorgehensweise zur Veröffentlichung von Basis-Images im Transfer Server-Repository vertraut. Siehe „Veröffentlichen von Paketdateien im Transfer Server-Repository“, auf Seite 305.

Vorgehensweise

1 Checken Sie die lokalen Linked-Clone-Desktops, die anhand des Basis-Images erstellt wurden, ein oder führen Sie ein Rollback für diese Desktops durch.

2 Initiieren Sie den Vorgang zur Neuzusammenstellung.

   Bei der Neuzusammenstellung werden Desktops im lokalen Modus ignoriert.

3 Veröffentlichen Sie das neu zusammengestellte Basis-Image im Transfer Server-Repository.

Die Linked-Clone-Desktops werden mit dem neuen Basis-Image aktualisiert.

Beim nächsten Auschecken der Linked-Clone-Desktops durch die Benutzer lädt View Transfer Server das aktualisierte Basis-Image aus dem Transfer Server-Repository auf die Clientcomputer herunter. View Transfer Server lädt auch die Betriebssystemfestplatten und die persistenten View Composer-Festplatten auf die Clientcomputer herunter.

Hinweis Desktops, die während der Neuzusammenstellung im lokalen Modus ausgeführt wurden, verwenden weiterhin das alte Basis-Image. Diese Desktops werden beim Einchecken durch die Benutzer nicht neu zusammengestellt.

Aktualisieren verknüpfter Klone bei der Desktop-Neuzusammenstellung

Bei einer Desktop-Neuzusammenstellung können Sie Betriebssystem-Patches bereitstellen, Anwendungen installieren bzw. aktualisieren oder die Desktop-Hardwareeinstellungen aller verknüpften Klone in einem Desktop-Pool ändern.

Für die Neuzusammenstellung von Linked-Clone-Desktops aktualisieren Sie die übergeordnete virtuelle Maschine in vCenter Server oder wählen eine andere virtuelle Maschine als neue übergeordnete Maschine aus. Anschließend erstellen Sie einen Snapshot der Konfiguration der neuen übergeordneten virtuellen Maschine.

Da die verknüpften Klone nicht direkt mit der übergeordneten virtuellen Maschine, sondern mit dem Replikat verknüpft sind, können Sie die übergeordnete virtuelle Maschine ändern, ohne dass sich dies auf die verknüpften Klone auswirkt.

Anschließend initiieren Sie die Neuzusammenstellung und wählen den Snapshot aus, der als neues Basis-Image für den Desktop-Pool verwendet werden soll. View Composer erstellt ein neues Replikat, kopiert die neu konfigurierte Betriebssystemfestplatte in die verknüpften Klone und koppelt die verknüpften Klone mit dem neuen Replikat.

Bei der Neuzusammenstellung werden auch die verknüpften Klone aktualisiert und die Größe der Betriebssystemfestplatten wird reduziert.

Desktop-Neuzusammenstellungen haben keine Auswirkungen auf persistente View Composer-Festplatten.

Befolgen Sie bei Neuzusammenstellungen die folgenden Richtlinien:

- Sie können Pools mit dedizierter und mit dynamischer Zuweisung neu zusammenstellen.
- Sie können einen Desktop-Pool nach Bedarf oder als geplantes Ereignis neu zusammenstellen.

  Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur eine Neuzusammenstellung planen. Bevor Sie eine Neuzusammenstellung planen können, müssen Sie alle zuvor geplanten Aufgaben abbrechen oder warten, bis der vorherige Vorgang abgeschlossen wurde. Um eine Neuzusammenstellung sofort zu starten, müssen Sie alle zuvor geplante Aufgaben abbrechen.

  Sie können mehrere Neuzusammenstellungen planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.
- Sie können ausgewählte verknüpfte Klone oder alle verknüpften Klone in einem Desktop-Pool neu zusammenstellen.
- Wenn verschiedene verknüpfte Klone in einem Pool von unterschiedlichen Snapshots des Basis-Images oder unterschiedlichen Basis-Images abgeleitet werden, umfasst der Pool mehrere Replikate.
- Sie können keine Desktops neu zusammenstellen, die im lokalen Modus ausgeführt werden. Lokale Desktops müssen eingecheckt werden, oder Sie müssen für diese Desktops ein Rollback durchführen, um den Vorgang zur Neuzusammenstellung ausführen zu können.
- Eine Neuzusammenstellung ist nur möglich, wenn die Benutzer sich von ihren View-Desktops abgemeldet haben.
- Sie können keine Neuzusammenstellung für verknüpfte Klone in eine neue oder aktualisierte übergeordnete virtuelle Maschine durchführen, die ein anderes Betriebssystem verwendet.
- Sie können keine Neuzusammenstellung für verknüpfte Windows 7-Klone mit einem bestimmten Betriebssystem-Festplattencontroller in eine neue oder aktualisierte übergeordnete virtuelle Maschine durchführen, die einen anderen Betriebssystem-Festplattencontroller verwendet.

- Sie können keine Neuzusammenstellung für verknüpfte Klone in eine Hardware-Version durchführen, die niedriger ist als die aktuelle Version. So können beispielsweise Klone mit der Hardware-Version 8 nicht in einer übergeordneten virtuellen Maschine neu zusammengestellt werden, die über die Hardware-Version 7 verfügt.

Hinweis Wenn Sie bei der Erstellung des Desktop-Pools zur Anpassung der verknüpften Klone eine Sysprep-Anpassungsspezifikation verwendet haben, werden für die neu zusammengestellten virtuellen Maschinen möglicherweise neue SIDs generiert. Weitere Informationen finden Sie unter „Neuzusammenstellung von mit Sysprep angepassten verknüpften Klonen“, auf Seite 102.

Korrigieren einer nicht erfolgreichen Neuzusammenstellung

Eine fehlgeschlagene Neuzusammenstellung kann korrigiert werden. Sie können zudem korrigierende Maßnahmen ergreifen, wenn Sie verknüpfte Klone versehentlich unter Verwendung eines falschen Basis-Images neu zusammenstellen.

Problem

Die Desktops weisen nach einer nicht erfolgreichen Neuzusammenstellung einen fehlerhaften oder veralteten Status auf.

Ursache

Möglicherweise ist während der Neuzusammenstellung auf dem vCenter Server-Host, in vCenter Server oder in einem Datenspeicher ein Systemfehler oder Problem aufgetreten.

Oder während der Neuzusammenstellung wurde ein VM-Snapshot mit einem anderen Betriebssystem verwendet als dem der ursprünglichen übergeordneten virtuellen Maschine. Beispiel: Sie haben möglicherweise einen Windows 7-Snapshot zur Neuzusammenstellung eines verknüpften Windows XP-Klons verwendet.

Lösung

1 Wählen Sie den Snapshot aus, der für die letzte erfolgreiche Neuzusammenstellung verwendet wurde.

  Sie können auch einen neuen Snapshot auswählen, um die verknüpften Klone mit einem neuen Status zu aktualisieren.

  Der Snapshot muss dasselbe Betriebssystem aufweisen wie der Snapshot der ursprünglichen übergeordneten virtuellen Maschine.

2 Stellen Sie den Pool erneut neu zusammen.

  View Composer erstellt anhand des Snapshots ein Basis-Image und erstellt die Linked-Clone-Betriebssystemfestplatten neu.

  Persistente View Composer-Festplatten mit Benutzerdaten und -einstellungen werden bei der Neuzusammenstellung beibehalten.

  Abhängig von den Bedingungen der nicht erfolgreichen Neuzusammenstellung können Sie die verknüpften Klone anstelle der oder zusätzlich zur Neuzusammenstellung aktualisieren oder neu verteilen.

  Hinweis Wenn Sie keine persistenten View Composer-Festplatten konfigurieren, werden die von Benutzern generierten Änderungen in den Linked-Clone-Desktops durch die Neuzusammenstellungen gelöscht.

Neuverteilen von Linked-Clone-Desktops

Bei einem Vorgang zur Neuverteilung für einen Desktop werden Linked-Clone-Desktops erneut auf die verfügbaren Datenspeicher verteilt.

Planen Sie Vorgänge zur Neuverteilung wenn möglich außerhalb der Spitzenzeiten.

Richtlinien finden Sie unter „Neuverteilung verknüpfter Klone auf logische Laufwerke“, auf Seite 240.

Voraussetzungen

- Machen Sie sich mit dem Vorgang zur Neuverteilung vertraut. Siehe „Neuverteilung verknüpfter Klone auf logische Laufwerke“, auf Seite 240.
- Legen Sie den Zeitpunkt für die Neuverteilung fest. Standardmäßig startet View Composer den Vorgang sofort.

  Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Neuverteilung planen. Sie können mehrere Vorgänge zur Neuverteilung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.
- Legen Sie fest, ob Sie das Abmelden aller Benutzer erzwingen möchten, sobald der Vorgang gestartet wird, oder ob gewartet werden soll, bis sich die einzelnen Benutzer abmelden, bevor für den Desktop des jeweiligen Benutzers eine Neuverteilung vorgenommen wird.

  Wenn Sie das Abmelden der Benutzer erzwingen, erhalten die Benutzer vor dem Trennen der Desktops eine Meldung von View Manager, sodass sie ihre Anwendungen schließen und sich abmelden können.
- Stellen Sie sicher, dass die Bereitstellung für den Pool aktiviert ist. Wenn die Bereitstellung für den Pool deaktiviert ist, verhindert View Manager eine Anpassung der Desktops nach deren Neuverteilung.
- Wenn Ihre Bereitstellung replizierte View Connection Server-Instanzen umfasst, überprüfen Sie, dass alle Instanzen in derselben Version vorliegen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Doppelklicken Sie zur Auswahl des Pools für die Neuverteilung in der linken Spalte auf die Pool-ID.

3 Legen Sie fest, ob der gesamte Pool oder nur ausgewählte Desktops neu verteilt werden sollen.

Option	Aktion
To rebalance all desktops in the pool (Neuverteilung aller Desktops im Pool)	Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Settings (Einstellungen)]** .
To rebalance selected desktops (Neuverteilung ausgewählter Desktops)	a Klicken Sie auf der Seite des ausgewählten Pools auf die Registerkarte **[Inventory (Bestandsliste)]** . b Wählen Sie die Desktops, für die eine Neuverteilung vorgenommen werden soll.

4 Klicken Sie auf **[View Composer] > [Rebalance (Neu verteilen)]** .

5 Befolgen Sie die Anweisungen des Assistenten, um für die Linked-Clone-Desktops eine Neuverteilung vorzunehmen.

Die Linked-Clone-Desktops werden aktualisiert und neu verteilt. Die ursprüngliche Größe der Betriebssystemfestplatten wird wiederhergestellt.

In View Administrator können Sie den Vorgang überwachen, indem Sie auf **[Inventory (Bestandsliste)] > [Pools]** klicken, die Pool-ID auswählen und anschließend auf die Registerkarte **[Tasks (Aufgaben)]** klicken. Zum Beenden, Anhalten oder Fortsetzen einer angehaltenen Aufgabe klicken Sie auf **[Cancel Task (Aufgabe abbrechen)]** , **[Pause Task (Aufgabe anhalten)]** oder **[Resume Task (Aufgabe fortsetzen)]** .

Neuverteilung verknüpfter Klone auf logische Laufwerke

Bei einem Vorgang zur Neuverteilung für einen Desktop werden Linked-Clone-Desktops erneut auf die verfügbaren logischen Laufwerke verteilt. Dadurch wird Speicherplatz auf überlasteten Laufwerken gespart und sichergestellt, dass Laufwerke optimal ausgelastet sind.

Wenn Sie große Linked-Clone-Desktop-Pools erstellen und mehrere LUNs (Logical Unit Number) verwenden, besteht das Risiko einer ineffizienten Speicherplatznutzung, wenn die anfängliche Größe nicht genau festgelegt wurde. Wird ein hoher Wert für die Speichermehrfachvergabe festgelegt, kann die Größe der verknüpften Klone rasch ansteigen, sodass der gesamte freie Speicherplatz im Datenspeicher möglicherweise schnell belegt ist.

Wenn die virtuellen Maschinen 95 % des Speicherplatzes im Datenspeicher belegen, generiert View Manager einen Warnungsprotokolleintrag. Bei einer Speicherbelegung von 99 % hält vSphere alle virtuellen Maschinen im Datenspeicher an.

Bei der Neuverteilung werden auch die verknüpften Klone aktualisiert und die Größe der Betriebssystemfestplatten wird reduziert. Dieser Vorgang hat keine Auswirkungen auf persistente View Composer-Festplatten.

Befolgen Sie bei Desktop-Neuverteilungen die folgenden Richtlinien:

- Sie können Pools mit dedizierter und mit dynamischer Zuweisung neu verteilen.
- Sie können ausgewählte verknüpfte Klone oder alle Klone in einem Pool neu verteilen.
- Sie können einen Desktop-Pool nach Bedarf oder als geplantes Ereignis neu verteilen.

  Sie können für eine Linked-Clone-Gruppe zu einem bestimmten Zeitpunkt jeweils nur einen Vorgang zur Neuverteilung planen. Wenn Sie eine Neuverteilung umgehend starten, setzt der Vorgang zuvor geplante Aufgaben außer Kraft.

  Sie können mehrere Vorgänge zur Neuverteilung planen, wenn sie sich auf verschiedene verknüpfte Klone beziehen.

  Bevor Sie einen Vorgang zur Neuverteilung planen, müssen Sie zuvor geplante Aufgaben abbrechen.
- Eine Neuverteilung kann nur für Desktops durchgeführt werden, deren Status **[Available (Verfügbar)]**, **[Error (Fehler)]** oder **[Customizing (Wird angepasst)]** lautet und für die weder Zeitpläne noch Aufhebungsvorgänge ausstehen.
- Als empfohlene Vorgehensweise sollten virtuelle Linked-Clone-Maschinen nicht mit anderen Typen virtueller Maschinen in einem Datenspeicher kombiniert werden. So kann View Composer alle virtuellen Maschinen im Datenspeicher neu verteilen.
- Wenn Sie einen Pool bearbeiten und den Host oder Cluster und die Datenspeicher ändern, auf denen verknüpfte Klone gespeichert werden, können Sie die verknüpften Klone nur dann neu verteilen, wenn der neu ausgewählte Host oder Cluster über Vollzugriff für die ursprünglichen und die neuen Datenspeicher verfügt. Alle Hosts im neuen Cluster müssen auf die ursprünglichen und neuen Datenspeicher zugreifen können.

  Beispielsweise könnten Sie einen Linked-Clone-Pool auf einem eigenständigen Host erstellen und einen lokalen Datenspeicher zum Speichern der Klone auswählen. Wenn Sie den Pool bearbeiten und einen Cluster und einen freigegebenen Datenspeicher auswählen, schlägt die Neuverteilung fehl, da die Hosts im Cluster nicht auf den ursprünglichen, lokalen Datenspeicher zugreifen können.

Dateinamen von Linked-Clone-Festplatten nach einer Neuverteilung

Wenn Sie Linked-Clone-Desktops neu verteilen, ändert vCenter Server die Dateinamen von persistenten View Composer-Festplatten und Festplatten für löschbare Dateien in verknüpften Klonen, die in einen neuen Datenspeicher verschoben werden.

Die ursprünglichen Dateinamen identifizieren den Festplattentyp. Die umbenannten Festplatten enthalten keine solche Kennzeichnung.

Eine ursprüngliche persistente Festplatte umfasst eine `user-disk`-Kennzeichnung: *`Desktop-Name`*`-vdm-user-disk-D-`*`ID`*`.vmdk`.

Eine ursprüngliche Festplatte für löschbare Dateien umfasst eine `disposable`-Kennzeichnung: *`Desktop-Name`*`-vdm-disposable-`*`ID`*`.vmdk`.

Wenn ein verknüpfter Klon nach einer Neuverteilung in einen neuen Datenspeicher verschoben wurde, verwendet vCenter Server die folgende gängige Dateinamenssyntax für beide Festplattentypen: *`Desktop-Name_n`*`.vmdk`.

Verwalten persistenter View Composer-Festplatten

Sie können eine persistente Festplatte von einem Linked-Clone-Desktop trennen und mit einem anderen verknüpften Klon verknüpfen. Mithilfe dieser Funktion können Sie Benutzerinformationen getrennt von den Linked-Clone-Desktops verwalten.

Persistente View Composer-Festplatten

Mit View Composer können Betriebssystemdaten und Benutzerinformationen auf separaten Festplatten in Linked-Clone-Desktops konfiguriert werden. View Composer behält die Benutzerinformationen auf der persistenten Festplatte bei, wenn die Betriebssystemdaten aktualisiert oder neu verteilt werden.

Eine persistente View Composer-Festplatte enthält Benutzereinstellungen und andere von den Benutzern generierte Daten. Sie erstellen persistente Festplatten, wenn Sie einen Linked-Clone-Desktop-Pool erstellen. Siehe „Arbeitsblatt zum Erstellen eines Linked-Clone-Desktop-Pools“, auf Seite 89.

Sie können eine persistente Festplatte vom zugehörigen Linked-Clone-Desktop trennen und die Festplatte im ursprünglichen Datenspeicher oder in einem anderen Datenspeicher platzieren. Nach dem Trennen der Festplatte wird die virtuelle Linked-Clone-Maschine gelöscht. Eine getrennte persistente Festplatte ist nicht länger mit einem Desktop verknüpft.

Sie können eine getrennte persistente Festplatte auf verschiedene Arten mit einem anderen Linked-Clone-Desktop verknüpfen. Dies bietet verschiedene Möglichkeiten:

- Beim Löschen eines verknüpften Klons können die Benutzerdaten beibehalten werden.
- Wenn ein Mitarbeiter das Unternehmen verlässt, kann ein anderer Mitarbeiter auf dessen Benutzerdaten zugreifen.
- Ein Benutzer mit mehreren Desktops kann die Benutzerdaten in einem einzigen Desktop konsolidieren.

- Wenn der Zugriff auf eine virtuelle Maschine in vCenter Server nicht länger möglich ist, die persistente Festplatte jedoch weiterhin intakt ist, können Sie die persistente Festplatte importieren und unter Verwendung dieser Festplatte einen neuen verknüpften Klon erstellen.

HINWEIS Sie können eine persistente Festplatte nicht von einem verknüpften Windows XP-Klon trennen und die persistente Festplatte für einen verknüpften Windows 7- oder Windows Vista-Klon neu erstellen oder mit diesem verknüpfen. Persistente Festplatten müssen mit dem Betriebssystem verbunden bleiben, das bei ihrer Erstellung verwendet wurde.

View Manager kann persistente Festplatten von Linked-Clone-Pools verwalten, die in View Manager 4.5 oder höher erstellt wurden. Persistente Festplatten, die in früheren Versionen von View Manager erstellt wurden, können nicht verwaltet werden und werden auf der Seite **[Persistent Disks (Persistente Festplatten)]** in View Administrator nicht angezeigt.

Trennen einer persistenten View Composer-Festplatte

Wenn Sie eine persistente View Composer-Festplatte von einem Linked-Clone-Desktop trennen, wird die Festplatte gespeichert und der verknüpfte Klon wird gelöscht. Indem Sie eine persistente Festplatte trennen, können Sie benutzerspezifische Informationen in einem anderen Desktop speichern und wiederverwenden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Persistente Festplatten]** .

2 Wählen Sie die zu trennende persistente Festplatte aus.

3 Klicken Sie auf **[Detach (Trennen)]** .

4 Legen Sie den Speicherort für die persistente Festplatte fest.

Option	Beschreibung
Use current datastore (Aktuellen Datenspeicher verwenden)	Zum Speichern der persistenten Festplatte im aktuellen Datenspeicher.
Move to the following datastore (In folgenden Datenspeicher verschieben)	Zum Auswählen eines neuen Datenspeichers für die persistente Festplatte. Klicken Sie auf **[Browse (Durchsuchen)]** und auf den nach unten weisenden Pfeil, um im Menü **[Choose a Datastore (Datenspeicher auswählen)]** einen neuen Datenspeicher auszuwählen.

Die persistente View Composer-Festplatte wird im Datenspeicher gespeichert. Der Linked-Clone-Desktop wird gelöscht und in View Administrator nicht mehr angezeigt.

Verknüpfen einer persistenten View Composer-Festplatte mit einem anderen Linked-Clone-Desktop

Sie können eine getrennte persistente Festplatte mit einem anderen Linked-Clone-Desktop verknüpfen. Nach dem Verknüpfen einer persistenten Festplatte sind die Benutzereinstellungen und -informationen auf der Festplatte für den Benutzer des anderen Desktops verfügbar.

Getrennte persistente Festplatten werden als sekundäre Festplatte mit dem ausgewählten Linked-Clone-Desktop verknüpft. Der Benutzer des neuen Desktops kann auf die sekundäre Festplatte und die vorhandenen Benutzerinformationen und -einstellungen auf dem Desktop zugreifen.

Voraussetzungen

Vergewissern Sie sich, dass der ausgewählte Desktop dasselbe Betriebssystem verwendet wie der verknüpfte Klon, in dem die persistente Festplatte erstellt wurde.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Persistente Festplatten]** .

2 Klicken Sie auf die Registerkarte **[Detached (Getrennt)]** .

3 Wählen Sie die persistente Festplatte aus.

4 Klicken Sie auf **[Attach (Verknüpfen)]** .

5 Wählen Sie einen Linked-Clone-Desktop aus, mit dem die persistente Festplatte verknüpft werden soll.

6 Wählen Sie **[Attach as a secondary disk (Als sekundäre Festplatte verknüpfen)]** .

7 Klicken Sie auf **[Finish (Fertig stellen)]** .

Weiter

Stellen Sie sicher, dass der Benutzer des Linked-Clone-Desktops über ausreichende Berechtigungen zur Verwendung der verknüpften sekundären Festplatte verfügt. Wenn der ursprüngliche Benutzer beispielsweise über bestimmte Zugriffsberechtigungen für die persistente Festplatte verfügte und diese auf dem neuen Desktop als Laufwerk `D` verknüpft ist, muss der neue Desktop-Benutzer über die Zugriffsberechtigungen des ursprünglichen Benutzers für Laufwerk `D` verfügen.

Melden Sie sich als Administrator am Gastbetriebssystem des Desktops an und weisen Sie dem neuen Desktop-Benutzer geeignete Berechtigungen zu.

Bearbeiten des Pools oder Benutzers einer persistenten View Composer-Festplatte

Sie können eine getrennte persistente View Composer-Festplatte einem neuen Pool oder Benutzer zuweisen, wenn der ursprüngliche Pool oder Benutzer aus View Manager gelöscht wurde.

Eine getrennte persistente Festplatte ist weiterhin mit dem ursprünglichen Pool und Benutzer verknüpft. Wenn der Pool oder Benutzer aus View Manager gelöscht wurde, können Sie die persistente Festplatte nicht zur Neuerstellung eines Linked-Clone-Desktops verwenden.

Indem Sie den Pool und Benutzer bearbeiten, können Sie die getrennte persistente Festplatte zur Neuerstellung eines Desktops im neuen Pool verwenden. Der Desktop wird dem neuen Benutzer zugewiesen.

Sie können einen neuen Pool, einen neuen Benutzer oder beides auswählen.

Voraussetzungen

- Vergewissern Sie sich, dass der Pool oder Benutzer der persistenten Festplatte aus View Manager gelöscht wurde.
- Vergewissern Sie sich, dass der neue Pool dasselbe Betriebssystem verwendet wie der Pool, in dem die persistente Festplatte erstellt wurde.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Persistent disks (Persistente Festplatten)]**

2 Wählen Sie die persistente Festplatte aus, deren Benutzer oder Pool gelöscht wurde.

3 Klicken Sie auf **[Edit (Bearbeiten)]** .

4 (Optional) Wählen Sie einen Linked-Clone-Pool aus der Liste aus.

5 (Optional) Wählen Sie einen Benutzer für die persistente Festplatte aus.

Sie können Active Directory nach der Domäne und dem Benutzernamen durchsuchen.

Weiter

Führen Sie eine Neuerstellung eines Linked-Clone-Desktops mit der getrennten persistenten Festplatte aus.

Neuerstellung eines Linked-Clone-Desktops mit getrennter persistenter Festplatte

Wenn Sie eine persistente View Composer-Festplatte trennen, wird der verknüpfte Klon gelöscht. Der ursprüngliche Benutzer kann auf die Benutzereinstellungen und -informationen auf der getrennten Festplatte zugreifen, indem Sie den Linked-Clone-Desktop basierend auf der getrennten Festplatte neu erstellen.

Hinweis Wenn Sie einen Linked-Clone-Desktop in einem Pool neu erstellen, dessen maximale Größe erreicht wurde, wird der Desktop dennoch zum Pool hinzugefügt. Die Größe des Pools überschreitet die angegebene maximale Größe.

Wenn der ursprüngliche Pool oder Benutzer einer persistenten Festplatte aus View Manager gelöscht wurde, kann der persistenten Festplatte ein neuer Pool oder Benutzer zugewiesen werden. Siehe „Bearbeiten des Pools oder Benutzers einer persistenten View Composer-Festplatte“, auf Seite 243.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Persistent disks (Persistente Festplatten)]** .

2 Klicken Sie auf die Registerkarte **[Detached (Getrennt)]** .

3 Wählen Sie die persistente Festplatte aus.

Sie können mehrere persistente Festplatten auswählen, um für jede Festplatte einen Linked-Clone-Desktop neu zu erstellen.

4 Klicken Sie auf **[Recreate Desktop (Desktop neu erstellen)]** .

5 Klicken Sie auf **[OK]** .

View Manager erstellt einen Linked-Clone-Desktop für jede ausgewählte persistente Festplatte und fügt den Desktop zum ursprünglichen Pool hinzu.

Die persistenten Festplatten werden weiterhin im ursprünglichen Datenspeicher gespeichert.

Wiederherstellen eines Linked-Clone-Desktops durch den Import einer persistenten Festplatte aus vSphere

Linked-Clone-Desktops, die mit einer persistenten View Composer-Festplatte konfiguriert wurden, können wiederhergestellt werden, wenn der Desktop in View Manager nicht länger verfügbar ist. Sie können die persistente Festplatte aus einem vSphere-Datenspeicher in View Manager importieren.

Die persistente Festplattendatei wird als getrennte persistente Festplatte in View Manager importiert. Sie können die getrennte Festplatte entweder mit einem vorhandenen Desktop verknüpfen oder den ursprünglichen verknüpften Klon in View Manager erneut erstellen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Persistent disks (Persistente Festplatten)]** .

2 Klicken Sie auf die Registerkarte **[Detached (Getrennt)]** .

3 Klicken Sie auf **[Import from vCenter (Aus vCenter importieren)]** .

4 Wählen Sie eine vCenter Server-Instanz.

5 Wählen Sie das Rechenzentrum, in dem sich die Festplattendatei befindet.

6 Wählen Sie einen Linked-Clone-Pool, in dem ein neuer Linked-Clone-Desktop mit der persistenten Festplatte erstellt werden soll.

7 Klicken Sie im Feld **[Persistent Disk File (Persistente Festplattendatei)]** auf **[Browse (Durchsuchen)]** und auf den nach unten weisenden Pfeil, um im Menü **[Choose a Datastore (Datenspeicher auswählen)]** einen Datenspeicher auszuwählen.

8 Klicken Sie auf den Datenspeichernamen, um die enthaltenen Festplattenspeicherdateien und Dateien virtueller Maschinen anzuzeigen.

9 Wählen Sie die zu importierende persistente Festplattendatei aus.

10 Klicken Sie im Feld **[User (Benutzer)]** auf **[Browse (Durchsuchen)]** , wählen Sie einen Benutzer zur Zuweisung zum Desktop aus, und klicken Sie auf **[OK]** .

Die Festplattendatei wird in View Manager als getrennte persistente Festplatte importiert.

Weiter

Um den Linked-Clone-Desktop wiederherzustellen, können Sie den ursprünglichen Desktop neu erstellen oder die getrennte persistente Festplatte mit einem anderen Desktop verknüpfen.

Weitere Informationen finden Sie unter „Neuerstellung eines Linked-Clone-Desktops mit getrennter persistenter Festplatte“, auf Seite 244 und „Verknüpfen einer persistenten View Composer-Festplatte mit einem anderen Linked-Clone-Desktop“, auf Seite 242.

Löschen einer getrennten persistenten View Composer-Festplatte

Wenn Sie eine getrennte persistente Festplatte löschen, können Sie die Festplatte entweder aus View Manager entfernen und im Datenspeicher beibehalten oder sowohl aus View Manager als auch aus dem Datenspeicher löschen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Persistent Disks (Persistente Festplatten)]** .

2 Klicken Sie auf die Registerkarte **[Detached (Getrennt)]** .

3 Wählen Sie die persistente Festplatte aus.

4 Klicken Sie auf **[Delete (Löschen)]** .

5 Legen Sie fest, ob die Festplatte nach dem Entfernen aus View Manager aus dem Datenspeicher gelöscht oder im Datenspeicher beibehalten werden soll.

Option	Beschreibung
Delete from disk (Von Festplatte löschen)	Die persistente Festplatte ist nach dem Löschvorgang nicht mehr vorhanden.
Delete from View Manager only (Nur aus View Manager löschen)	Die persistente Festplatte ist nach dem Löschvorgang in View Manager nicht mehr verfügbar, im Datenspeicher jedoch weiterhin vorhanden.

6 Klicken Sie auf **[OK]** .

Verwalten von Desktops und Desktop-Pools 11

Sie können Desktop-Pools, VM-Desktops und Desktop-Sitzungen in View Administrator verwalten.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwalten von Desktop-Pools“, auf Seite 247
- „Reduzieren der Adobe Flash-Bandbreite“, auf Seite 253
- „Verwalten von VM-Desktops“, auf Seite 255
- „Exportieren von View-Informationen in externe Dateien“, auf Seite 260

Verwalten von Desktop-Pools

Sie können Desktop-Pools in View Administrator bearbeiten, deaktivieren und löschen.

Bearbeiten eines Desktop-Pools

Sie können einen vorhandenen Desktop-Pool bearbeiten, um Einstellungen wie Pool-Einstellungen, die Anzahl an Reserve-Desktops, Datenspeicher und Anpassungsspezifikationen zu konfigurieren.

Voraussetzungen

Machen Sie sich mit den Pool-Einstellungen vertraut, die nach der Pool-Erstellung geändert bzw. nicht geändert werden können. Siehe „Ändern der Einstellungen in einem vorhandenen Desktop-Pool“, auf Seite 248 und „Feste Einstellungen in einem vorhandenen Desktop-Pool“, auf Seite 248.

Vorgehensweise

1 Klicken Sie auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Wählen Sie einen Pool aus.

3 Klicken Sie auf **[Edit (Bearbeiten)]** .

4 Klicken Sie im Dialogfeld **[Edit (Bearbeiten)*Pool-Name*]** auf eine Registerkarte und konfigurieren Sie die Pool-Optionen neu.

5 Klicken Sie auf **[OK]** .

Ändern der Einstellungen in einem vorhandenen Desktop-Pool

Nach dem Erstellen eines Desktop-Pools können bestimmte Konfigurationseinstellungen geändert werden.

Tabelle 11-1. Bearbeitbare Einstellungen in einem vorhandenen Desktop-Pool

Registerkarte "Configuration (Konfiguration)"	Beschreibung
[General (Allgemein)]	Bearbeiten von Optionen für die Pool-Benennung.
[Pool Settings (Pool-Einstellungen)]	Bearbeiten von Desktop-Einstellungen, z. B. die Remote-Desktop-Betriebsrichtlinie, das Anzeigeprotokoll und Adobe Flash-Einstellungen.
[Provisioning Settings (Bereitstellungseinstellungen)]	Bearbeiten von Optionen für die Pool-Bereitstellung und Hinzufügen von Desktops zum Pool. Diese Registerkarte ist nur für automatisierte Pools verfügbar.
[vCenter Settings (vCenter-Einstellungen)]	Bearbeiten der VM-Vorlage oder des standardmäßigen Basis-Images. Hinzufügen oder Ändern von vCenter Server-Instanzen, ESX-Hosts oder -Clustern, Datenspeichern und anderen vCenter-Funktionen. Die neuen Werte wirken sich nur auf neue virtuelle Maschinen aus, die nach dem Ändern der Einstellungen erstellt werden. Die neuen Einstellungen haben keine Auswirkungen auf vorhandene virtuelle Maschinen. Diese Registerkarte ist nur für automatisierte Pools verfügbar.
[Guest Customization (Gastanpassung)]	Auswählen von Sysprep-Anpassungsspezifikationen. Wenn für die Anpassung eines Linked-Clone-Pools QuickPrep verwendet wurde, können Sie die Active Directory-Domäne und den Active Directory-Container ändern und QuickPrep-Abschaltskripts sowie nach der Synchronisierung ausgeführte Skripts angeben. Diese Registerkarte ist nur für automatisierte Pools verfügbar.

Feste Einstellungen in einem vorhandenen Desktop-Pool

Nach dem Erstellen eines Desktop-Pools können bestimmte Konfigurationseinstellungen nicht geändert werden.

Tabelle 11-2. Feste Einstellungen in einem vorhandenen Desktop-Pool

Einstellung	Beschreibung
Pool type (Pool-Typ)	Nach der Erstellung eines automatisierten, manuellen oder Terminaldienste-Pools kann der Pool-Typ nicht geändert werden.
User assignment (Benutzerzuweisung)	Ein Wechsel zwischen dedizierten und dynamischen Zuweisungen ist nicht möglich.
Type of virtual machine (Typ der virtuellen Maschine)	Ein Wechsel zwischen vollständigen Desktops und Linked-Clone-Desktops ist nicht möglich.
Pool ID (Pool-ID)	Die Pool-ID kann nicht geändert werden.
Desktop-naming and provisioning method (Benennungs- und Bereitstellungsmethode für Desktop)	Zum Hinzufügen von Desktops zu einem Pool muss die Bereitstellungsmethode verwendet werden, die zur Erstellung des Pools verwendet wurde. Ein Wechsel zwischen der manuellen Angabe von Desktop-Namen und der Verwendung eines Benennungsmusters ist nicht möglich. Bei der manuellen Angabe von Namen können Namen zur Liste der Desktop-Namen hinzugefügt werden. Bei Verwendung eines Benennungsmusters kann die maximale Anzahl an Desktops erhöht werden.

Tabelle 11-2. Feste Einstellungen in einem vorhandenen Desktop-Pool (Fortsetzung)

Einstellung	Beschreibung
vCenter settings (vCenter-Einstellungen)	vCenter-Einstellungen für vorhandene virtuelle Maschinen können nicht geändert werden. Sie können vCenter-Einstellungen im Dialogfeld **[Edit (Bearbeiten)*Pool-Name*]** ändern, die Werte gelten jedoch nur für virtuelle Maschinen, die nach dem Ändern der Einstellungen erstellt werden.
View Composer, persistente Festplatten	Nach der Erstellung eines Linked-Clone-Pools ohne persistente Festplatten können keine persistenten Festplatten konfiguriert werden.
View Composer customization method (View Composer-Anpassungsmethode)	Nach der Anpassung eines Linked-Clone-Pools mit QuickPrep oder Sysprep können Sie nicht zur anderen Anpassungsmethode wechseln, wenn Sie Desktops im Pool erstellen oder neu zusammenstellen.

Ändern der Größe eines automatisierten Pools, der über ein Benennungsmuster bereitgestellt wurde

Wenn Sie einen automatisierten Desktop-Pool über ein Benennungsmuster bereitstellen, können Sie die Größe des Pools erhöhen oder verringern, indem Sie die maximale Anzahl an Desktops ändern.

Voraussetzungen

- Stellen Sie sicher, dass der Pool über ein Benennungsmuster bereitgestellt wurde. Weitere Informationen zur manuellen Angabe von Desktop-Namen finden Sie unter „Hinzufügen von Desktops zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde“, auf Seite 250.
- Stellen Sie sicher, dass der Pool automatisiert ist.

Vorgehensweise

1. Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .
2. Wählen Sie den Pool aus und klicken Sie auf **[Edit (Bearbeiten)]** .
3. Klicken Sie auf die Registerkarte **[Provisioning Settings (Bereitstellungseinstellungen)]** .
4. Geben Sie im Feld **[Max number of desktops (Maximale Anzahl an Desktops)]** die neue Anzahl an Desktops im Pool an.

Wenn Sie die Pool-Größe erhöhen, können so lange neue Desktops zum Pool hinzugefügt werden, bis die maximale Anzahl erreicht ist.

Beim Verringern der Größe eines Pools mit dynamischer Zuweisung werden nicht verwendete Desktops gelöscht. Wenn mehr Benutzer am Pool angemeldet sind als der neue Höchstwert, wird die Pool-Größe nach dem Abmelden der Benutzer verringert.

Beim Verringern der Größe eines Pools mit dedizierter Zuweisung werden nicht zugewiesene Desktops gelöscht. Wenn dem Desktop mehr Benutzer zugewiesen sind als der neue Höchstwert, wird die Pool-Größe nach dem Aufheben von Benutzerzuweisungen verringert.

Hinweis Beim Verringern der Pool-Größe kann die tatsächliche Anzahl an Desktops größer sein als der Wert von **[Max number of desktops (Maximale Anzahl an Desktops)]** , wenn gegenwärtig mehr Benutzer angemeldet oder den Desktops zugewiesen sind als dieser festgelegte Höchstwert.

Hinzufügen von Desktops zu einem automatisierten Pool, der über eine Namensliste bereitgestellt wurde

Zum Hinzufügen von Desktops zu einem automatisierten Pool, für dessen Bereitstellung manuell Desktop-Namen angegeben wurden, stellen Sie eine alternative Liste mit neuen Desktop-Namen bereit. Mit dieser Funktion können Sie einen Desktop-Pool erweitern und weiterhin die Benennungskonventionen Ihres Unternehmens verwenden.

Befolgen Sie beim manuellen Hinzufügen von Desktop-Namen die folgenden Richtlinien:

- Geben Sie jeden Desktop-Namen in einer separaten Zeile ein.
- Ein Desktop-Name kann bis zu 15 alphanumerische Zeichen umfassen.
- Sie können jedem Desktop-Eintrag einen Benutzernamen hinzufügen. Mithilfe eines Kommas können Sie den Benutzernamen vom Desktop-Namen trennen.

In diesem Beispiel werden zwei Desktops hinzugefügt. Der zweite Desktop ist mit einem Benutzer verknüpft:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

Hinweis In einem Pool mit dynamischer Zuweisung können keine Benutzernamen mit Desktop-Namen verknüpft werden. Die Desktops werden den verknüpften Benutzern nicht dediziert zugewiesen. In einem Pool mit dynamischer Zuweisung bleiben alle derzeit ungenutzten Desktops jedem Benutzer zugänglich, der sich anmeldet.

Voraussetzungen

Stellen Sie sicher, dass der Pool durch die manuelle Angabe von Desktop-Namen erstellt wurde. Wenn der Pool über die Bereitstellung eines Benennungsmusters erstellt wurde, können Pools nicht über die manuelle Angabe von neuen Desktop-Namen hinzugefügt werden.

Vorgehensweise

1 Erstellen Sie eine Textdatei mit der Liste zusätzlicher Desktop-Namen.

   Wenn nur einige wenige Desktops hinzugefügt werden sollen, können Sie die Desktop-Namen direkt im Assistenten zum Hinzufügen eines Pools eingeben. Sie müssen keine separate Textdatei erstellen.

2 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

3 Wählen Sie den zu erweiternden Pool aus.

4 Klicken Sie auf **[Edit (Bearbeiten)]** .

5 Klicken Sie auf die Registerkarte **[Provisioning Settings (Bereitstellungseinstellungen)]** .

6 Klicken Sie auf **[Add Desktops (Desktops hinzufügen)]** .

7 Kopieren Sie Ihre Liste mit Desktop-Namen in die Seite **[Enter Desktop Names (Desktop-Namen eingeben)]** , und klicken Sie auf **[Next (Weiter)]** .

   Der Assistent zum Eingeben von Desktop-Namen zeigt die Desktop-Liste an und weist mit einem roten **[X]** auf Validierungsfehler hin.

8 Korrigieren Sie ungültige Desktop-Namen.

   a Platzieren Sie Ihren Cursor auf einem ungültigen Namen, um die entsprechende Fehlermeldung im unteren Seitenbereich anzuzeigen.

   b Klicken Sie auf **[Back (Zurück)]** .

   c Bearbeiten Sie die fehlerhaften Namen, und klicken Sie auf **[Next (Weiter)]** .

9 Klicken Sie auf **[Finish (Fertig stellen)]** .

10 Klicken Sie auf **[OK]** .

View Manager fügt die neuen Desktops zum Pool hinzu.

Die Erstellung der neuen virtuellen Maschinen kann in vCenter Server überwacht werden.

In View Administrator können Sie die Desktops so anzeigen, wie sie dem Pool hinzugefügt werden. Klicken Sie hierzu auf **[Inventory (Bestandsliste)] > [Pools]** oder **[Inventory (Bestandsliste)] > [Desktops]** .

Deaktivieren oder Aktivieren eines Desktop-Pools

Wenn Sie einen Desktop-Pool deaktivieren, wird der Pool den Benutzern nicht mehr angezeigt und die Pool-Bereitstellung wird gestoppt. Benutzer haben keinen Zugriff auf den Pool. Ein deaktivierter Pool kann erneut aktiviert werden.

Sie können einen Pool deaktivieren, um Benutzer am Zugriff auf ihre Desktops zu hindern, während Sie die Desktops für ihre Verwendung vorbereiten. Wenn ein Pool nicht länger benötigt wird, können Sie den Pool durch eine Deaktivierung außer Betrieb nehmen, ohne die Pool-Definition aus View Manager löschen zu müssen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie einen Desktop-Pool aus und ändern Sie den Status des Pools.

Option	Aktion
Deaktivieren des Pools	Klicken Sie auf **[Status] > [Disable Pool (Pool deaktivieren)]** .
Aktivieren des Pools	Klicken Sie auf **[Status] > [Enable Pool (Pool aktivieren)]** .

3 Klicken Sie auf **[OK]** .

Deaktivieren oder Aktivieren der Bereitstellung in einem Desktop-Pool

Wenn Sie die Bereitstellung in einem Desktop-Pool deaktivieren, stellt View Manager das Bereitstellen neuer virtueller Maschinen für den Pool ein. Die Bereitstellung kann erneut aktiviert werden, nachdem sie deaktiviert wurde.

Bevor Sie die Konfiguration eines Pools ändern, können Sie die Bereitstellung deaktivieren. Auf diese Weise ist sichergestellt, dass keine neuen Desktops mit der alten Konfiguration erstellt werden. Sie können die Bereitstellung auch deaktivieren, um View Manager an der Belegung von zusätzlichem Speicherplatz zu hindern, wenn ein Pool den verfügbaren Speicherplatz fast vollständig ausgeschöpft hat.

Wenn in einem Linked-Clone-Pool die Bereitstellung deaktiviert ist, stellt View Manager die Bereitstellung neuer Desktops ein und verhindert die Anpassung von Desktops, nachdem diese neu zusammengestellt oder neu verteilt wurden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie einen Desktop-Pool aus und ändern Sie den Status des Pools.

Option	Aktion
Deaktivieren der Bereitstellung	Klicken Sie auf **[Status] > [Disable Provisioning (Deaktivieren der Bereitstellung)]** .
Aktivieren der Bereitstellung	Klicken Sie auf **[Status] > [Enable Provisioning (Aktivieren der Bereitstellung)]** .

3 Klicken Sie auf **[OK]** .

Löschen eines Desktop-Pools aus View Manager

Wenn Sie einen Desktop-Pool aus View Manager löschen, können die Benutzer nicht länger auf die Desktops innerhalb des Pools zugreifen.

Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, können Benutzer mit derzeit aktiven Sitzungen Desktops auf Grundlage vollständiger virtueller Maschinen weiterhin verwenden. Nach der Abmeldung der Benutzer können diese nicht länger auf die gelöschten Desktops zugreifen.

Bei Linked-Clone-Desktops löscht vCenter Server die virtuellen Maschinen immer von der Festplatte.

WICHTIG Löschen Sie die virtuellen Maschinen in vCenter Server erst, wenn Sie einen Desktop-Pool mit View Administrator gelöscht haben. Anderenfalls könnte dies dazu führen, dass die View-Komponenten einen inkonsistenten Status aufweisen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie einen Desktop-Pool aus und klicken Sie auf **[Delete (Löschen)]** .

3 Wählen Sie, wie der Pool gelöscht werden soll.

Option	Beschreibung
Pool that contains full virtual-machine desktops (Pool mit Desktops auf Grundlage vollständiger virtueller Maschinen)	Legen Sie fest, ob die virtuellen Maschinen in vCenter Server beibehalten oder gelöscht werden sollen. Wenn Sie die virtuellen Maschinen von der Festplatte löschen, werden Benutzer mit aktiven Sitzungen von ihren Desktops getrennt. Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, legen Sie fest, ob Benutzer mit aktiven Sitzungen mit ihren Desktops verbunden bleiben oder getrennt werden sollen.
Linked-clone pool with View Composer persistent disks (Linked-Clone-Pool mit persistenten View Composer-Festplatten)	Legen Sie fest, ob die persistenten Festplatten nach dem Löschen des Desktops getrennt oder gelöscht werden sollen. In beiden Fällen löscht vCenter Server die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit gegenwärtig aktiven Sitzungen werden von ihren Linked-Clone-Desktops getrennt. Wenn Sie eine persistente Festplatte trennen, kann sie mit einem anderen Desktop verknüpft werden. Getrennte persistente Festplatten können in demselben Datenspeicher oder in einem anderen Datenspeicher platziert werden.
Linked-clone pool without View Composer persistent disks (Linked-Clone-Pool ohne persistente View Composer-Festplatten)	vCenter Server löscht die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit gegenwärtig aktiven Sitzungen werden von ihren Linked-Clone-Desktops getrennt.

Der Desktop-Pool wird aus View Connection Server entfernt. Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, kann View Manager nicht darauf zugreifen.

Beim Löschen von Desktop-Pools aus View Manager werden Linked-Clone-Computerkonten aus Active Directory entfernt. Die Konten vollständiger virtueller Maschinen sind weiterhin in Active Directory vorhanden. Diese Konten müssen manuell aus Active Directory entfernt werden.

Beim Löschen von Pools mit lokalen Desktops werden die Rechenzentrumskopien der Desktops aus View Manager entfernt. Die lokalen Desktops sind nicht mehr funktionsfähig, wenn die Clients View Connection Server kontaktieren oder die maximale Dauer ohne Serverkontakt überschritten wird. Wenn Sie festlegen, dass vollständige virtuelle Maschinen in vCenter Server beibehalten werden, oder wenn Sie persistente View Composer-Festplatten trennen und speichern, werden Benutzeränderungen an lokalen Desktops seit der letzten Replikation oder seit dem letzten Auschecken nicht auf den virtuellen Maschinen oder persistenten Festplatten beibehalten.

Reduzieren der Adobe Flash-Bandbreite

Sie können die durch Adobe Flash-Inhalte in View-Desktop-Sitzungen verwendete Bandbreite reduzieren. Durch diese Reduzierung kann die Browsing-Leistung insgesamt sowie die Reaktionsfähigkeit anderer im Desktop ausgeführten Anwendungen verbessert werden.

Konfigurieren der Adobe Flash-Qualität und -Drosselung

Sie können Modi für die Adobe Flash-Qualität und -Drosselung festlegen, um die von Adobe Flash-Inhalten in View-Desktops verwendete Bandbreite zu reduzieren.

Voraussetzungen

Machen Sie sich mit den Adobe Flash-Qualitäts- und Drosselungseinstellungen vertraut. Siehe „Adobe Flash-Qualität und -Drosselung“, auf Seite 253.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Pools]** .

2 Wählen Sie einen Pool aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Klicken Sie auf die Registerkarte **[Pool Settings (Pool-Einstellungen)]** .

4 Wählen Sie im Menü **[Adobe Flash quality (Adobe Flash-Qualität)]** einen Qualitätsmodus aus.

5 Wählen Sie im Menü **[Adobe Flash throttling (Adobe Flash-Drosselung)]** einen Drosselungsmodus aus.

6 Klicken Sie auf **[OK]** .

Hinweis Die Einstellungen zur Reduzierung der Adobe Flash-Bandbreitennutzung werden erst angewendet, wenn View Client erneut eine Verbindung mit dem Desktop herstellt.

Adobe Flash-Qualität und -Drosselung

Sie können die höchste zulässige Qualitätsstufe für Adobe Flash-Inhalte festlegen, welche die Webseiteneinstellungen außer Kraft setzt. Wenn die Adobe Flash-Qualität für eine Webseite höher ist als die zulässige maximale Qualitätsstufe, wird die Qualität auf den angegebenen Höchstwert reduziert. Eine geringere Qualität führt zu größeren Bandbreiteeinsparungen.

Um die Einstellungen zur Reduzierung der Adobe Flash-Bandbreite zu nutzen, darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

Tabelle 11-3 zeigt die verfügbaren Einstellungen für die Adobe Flash-Anzeigequalität.

Tabelle 11-3. Adobe Flash-Qualitätseinstellungen

Qualitätseinstellung	Beschreibung
[Do not control (Keine Festlegung)]	Die Qualität wird durch die Webseiteneinstellungen bestimmt.
[Low (Niedrig)]	Mit dieser Einstellung werden die höchsten Bandbreiteeinsparungen erzielt.

Tabelle 11-3. Adobe Flash-Qualitätseinstellungen (Fortsetzung)

Qualitätseinstellung	Beschreibung
[Medium (Mittel)]	Mit dieser Einstellung werden mittlere Bandbreiteeinsparungen erzielt.
[High (Hoch)]	Mit dieser Einstellung werden die geringsten Bandbreiteeinsparungen erzielt.

Wird keine maximale Qualitätsstufe angegeben, lautet der Standardwert des Systems **[Low (Niedrig)]**

Adobe Flash verwendet Zeitgeberdienste, um die Bildschirmanzeige zu aktualisieren. Ein typischer Wert für ein Adobe Flash-Zeitgeberintervall ist 4 bis 50 Millisekunden. Durch die Drosselung bzw. Verlängerung des Intervalls kann die Frame-Rate und damit die Bandbreitennutzung reduziert werden.

Tabelle 11-4 zeigt die verfügbaren Einstellungen für die Adobe Flash-Drosselung.

Tabelle 11-4. Adobe Flash-Drosselungseinstellungen

Drosselungseinstellung	Beschreibung
[Disabled (Deaktiviert)]	Es erfolgt keine Drosselung. Das Zeitgeberintervall bleibt unverändert.
[Conservative (Konservativ)]	Das Zeitgeberintervall lautet 100 Millisekunden. Diese Einstellung führt zur geringsten Anzahl an verworfenen Frames.
[Moderate (Mittel)]	Das Zeitgeberintervall lautet 500 Millisekunden.
[Aggressive (Aggressiv)]	Das Zeitgeberintervall lautet 2500 Millisekunden. Diese Einstellung führt zur höchsten Anzahl an verworfenen Frames.

Die Audiogeschwindigkeit bleibt unabhängig von der gewählten Drosselungseinstellung konstant.

Konfigurieren der Adobe Flash-Drosselung in Internet Explorer für Terminaldienste-Sitzungen

Um sicherzustellen, dass die Adobe Flash-Drosselung in Internet Explorer für Terminaldienste-Sitzungen funktioniert, müssen die Benutzer Browsererweiterungen von Drittanbietern aktivieren.

Vorgehensweise

1 Starten Sie View Client und melden Sie sich an einem Benutzer-Desktop an.

2 Klicken Sie in Internet Explorer auf **[Tools (Extras)]** > **[Internet Options (Internetoptionen)]** .

3 Klicken Sie auf die Registerkarte **[Advanced (Erweitert)]** , wählen Sie **[Enable third-party browser extensions (Browsererweiterungen von Drittanbietern aktivieren)]** und klicken Sie auf **[OK]** .

4 Starten Sie Internet Explorer neu.

Außerkraftsetzen der Einstellungen zur Bandbreitenreduzierung im Desktop

Benutzer können die Anzeigeeinstellungen für Adobe Flash-Inhalte im Desktop mithilfe des Mauscursors außer Kraft setzen.

Vorgehensweise

1 Starten Sie auf einem View-Desktop den Internet Explorer und navigieren Sie zum relevanten Adobe Flash-Inhalt.

Starten Sie den Inhalt gegebenenfalls.

Je nach Konfiguration der Adobe Flash-Einstellungen ist die Wiedergabequalität möglicherweise verringert.

2 Bewegen Sie den Mauscursor während der Wiedergabe in die Adobe Flash-Inhalte.

Die Anzeigequalität wird verbessert, solange sich der Cursor innerhalb der Adobe Flash-Inhalte befindet.

3 Doppelklicken Sie in die Adobe Flash-Inhalte, um die verbesserte Wiedergabequalität beizubehalten.

Verwalten von VM-Desktops

Sie können VM-Desktops suchen, verwalten und löschen sowie Desktop-Sitzungen verwalten.

Anzeigen, Trennen oder Neustarten aktiver Sitzungen

Sie können die Benutzer mit aktiven Verbindungen zu den View-Desktops in einem Pool anzeigen. Sie können Benutzer von ihren Desktops trennen, die Abmeldung der Benutzer erzwingen und die aktiven Sitzungen neu starten.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pool]** .

2 Doppelklicken Sie auf einen Pool und anschließend auf die Registerkarte **[Sessions (Sitzungen)]** .

3 Wählen Sie einen Desktop aus.

4 Wählen Sie, ob die Desktops getrennt, die Benutzer abgemeldet oder die Sitzung neu gestartet werden soll.

Option	Beschreibung
Disconnect Session (Sitzung trennen)	Trennt den Benutzer vom Desktop. Die Sitzung bleibt aktiv. Wenn **[Automatically logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)]** auf **[Never (Nie)]** festgelegt ist oder die angegebene Zeitdauer nach dem Trennen nicht überschritten wurde, kann sich der Benutzer erneut an der Sitzung anmelden. Die Einstellung **[Automatically logoff after disconnect (Nach Verbindungstrennung automatisch abmelden)]** kann beim Erstellen des Pools konfiguriert oder nach der Pool-Erstellung bearbeitet werden.
Logoff Session (Von Sitzung abmelden)	Trennt den Benutzer vom Desktop. Der Benutzer wird abgemeldet.
Reset (Zurücksetzen)	Fährt den Desktop herunter und startet die Sitzung ohne ordnungsgemäße Abmeldung und Trennung der Verbindung neu.
Send Message (Nachricht senden)	Ermöglicht die Eingabe einer Nachricht, die auf dem Desktop des Benutzers angezeigt wird.

Zuweisen eines Desktops zu einem Benutzer

In einem Pool mit dedizierter Zuweisung kann ein Benutzer als der Besitzer eines Desktops zugewiesen werden. Nur der zugewiesene Benutzer kann sich anmelden und eine Verbindung mit dem Desktop herstellen.

View Manager weist Benutzern in den folgenden Situationen Desktops zu.

- Wenn Sie einen Pool erstellen und die Einstellung **[Enable automatic assignment (Automatische Zuweisung aktivieren)]** auswählen.

  Hinweis Bei Auswahl der Einstellung **[Enable automatic assignment (Automatische Zuweisung aktivieren)]** können Benutzern weiterhin manuell Desktops zugewiesen werden.

- Wenn Sie einen automatisierten Pool erstellen, die Einstellung **[Specify desktop names manually (Desktop-Namen manuell angeben)]** auswählen und mit den Desktop-Namen Benutzernamen angeben.

Wenn Sie für einen Pool mit dedizierter Zuweisung keine der beiden Einstellungen festlegen, können die Benutzer nicht auf die Desktops zugreifen. In diesem Fall muss jedem Benutzer manuell ein Desktop zugewiesen werden.

Desktops können Benutzern auch mithilfe des Befehls `vdmadmin` zugewiesen werden. Siehe „Zuweisen von dedizierten Desktops unter Verwendung der Option „-L““, auf Seite 391.

Voraussetzungen

- Stellen Sie sicher, dass der Desktop zu einem Pool mit dedizierter Zuweisung gehört. Pool-Zuweisungen werden in View Administrator im Fenster des Desktop-Pools auf der Registerkarte **[Settings (Einstellungen)]** angezeigt.
- Stellen Sie sicher, dass der Desktop nicht zur Verwendung im lokalen Modus ausgecheckt ist. Sie können Benutzer nicht zuweisen und Benutzerzuweisungen nicht entfernen, während Desktops ausgecheckt sind.

Vorgehensweise

1. Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Desktops]** oder klicken Sie auf **[Inventory (Bestandsliste)]** > **[Pools]** . Doppelklicken Sie anschließend auf eine Pool-ID und wählen Sie die Registerkarte **[Inventory (Bestandsliste)]** .
2. Wählen Sie den Desktop aus.
3. Klicken Sie auf **[More Commands (Weitere Befehle)]** > **[Assign User (Benutzer zuweisen)]** .
4. Wählen Sie, ob nach Benutzern oder nach Gruppen gesucht werden soll, wählen Sie eine Domäne und geben Sie im Textfeld **[Name]** oder **[Description (Beschreibung)]** eine Suchzeichenfolge ein.
5. Wählen Sie den Benutzer- oder Gruppennamen und klicken Sie auf **[OK]** .

Aufheben der Benutzerzuweisung für einen dedizierten Desktop

In einem Pool mit dedizierter Zuweisung kann die Desktop-Zuweisung eines Benutzers entfernt werden.

Der Befehl `vdmadmin` kann ebenfalls verwendet werden, um die Zuweisung eines Desktops zu einem Benutzer zu entfernen. Siehe „Zuweisen von dedizierten Desktops unter Verwendung der Option „-L““, auf Seite 391.

Voraussetzungen

Stellen Sie sicher, dass der Desktop nicht zur Verwendung im lokalen Modus ausgecheckt ist. Sie können Benutzer nicht zuweisen und Benutzerzuweisungen nicht entfernen, während Desktops ausgecheckt sind.

Vorgehensweise

1. Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Desktops]** oder klicken Sie auf **[Inventory (Bestandsliste)]** > **[Pools]** . Doppelklicken Sie anschließend auf eine Pool-ID und wählen Sie die Registerkarte **[Inventory (Bestandsliste)]** .
2. Wählen Sie den Desktop aus.
3. Klicken Sie auf **[More Commands (Weitere Befehle)]** > **[Unassign User (Benutzerzuweisung aufheben)]** .
4. Klicken Sie auf **[OK]** .

Der Desktop ist verfügbar und kann einem anderen Benutzer zugewiesen werden.

Anpassen von vorhandenen Desktops im Wartungsmodus

Nach der Erstellung eines Desktop-Pools können einzelne Desktops angepasst, geändert oder getestet werden, indem Sie sie in den Wartungsmodus versetzen. Wenn sich ein Desktop im Wartungsmodus befindet, können die Benutzer nicht darauf zugreifen.

Vorhandene Desktops werden nacheinander in den Wartungsmodus versetzt. Der Wartungsmodus mehrerer Desktops kann in einem Vorgang beendet werden.

Beim Erstellen eines Pools können Sie alle Desktops in diesem Pool im Wartungsmodus starten, wenn Sie die Desktop-Namen manuell angeben. Weitere Informationen finden Sie unter „Anpassen von Desktops im Wartungsmodus“, auf Seite 125.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)] > [Desktops]** oder klicken Sie auf **[Inventory (Bestandsliste)] > [Pools]** . Doppelklicken Sie anschließend auf eine Pool-ID und wählen Sie die Registerkarte **[Inventory (Bestandsliste)]** .

2 Wählen Sie einen Desktop aus.

3 Klicken Sie auf **[More Commands (Weitere Befehle)] > [Enter Maintenance Mode (In Wartungsmodus wechseln)]** .

4 Passen Sie den VM-Desktop an oder ändern bzw. testen Sie ihn.

5 Wiederholen Sie die Schritte unter Schritt 2 bis Schritt 4 für alle Desktops, die Sie anpassen möchten.

6 Wählen Sie die angepassten Desktops aus und klicken Sie auf **[More Commands (Weitere Befehle)] > [Exit Maintenance Mode (Wartungsmodus beenden)]** .

Die geänderten Desktops sind nun für die Benutzer verfügbar.

Überwachen des Desktop-Status

Sie können den Status von Desktops in einer View-Bereitstellung problemlos über das View Administrator-Dashboard überwachen. Beispielsweise können alle getrennten Desktops oder alle Desktops im Wartungsmodus angezeigt werden.

Voraussetzungen

Machen Sie sich mit den Desktop-Status vertraut. Siehe „Desktop-Status virtueller Maschinen“, auf Seite 258.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Dashboard]** .

2 Erweitern Sie im Fenster **[Desktop Status (Desktop-Status)]** einen Statusordner.

Option	Beschreibung
Preparing (In Vorbereitung)	Listet die Desktop-Status auf, während die virtuelle Maschine bereitgestellt oder gelöscht wird bzw. sich im Wartungsmodus befindet.
Problem Desktops (Problematische Desktops)	Listet die Desktop-Fehlerstatus auf.
Prepared for use (Für die Verwendung vorbereitet)	Listet die Desktop-Status auf, wenn der Desktop verwendet werden kann.

3 Ermitteln Sie den Desktop-Status und klicken Sie auf die neben dem Status angezeigte Hyperlink-Nummer.

Auf der Seite **[Desktops]** werden alle Desktops mit dem ausgewählten Status angezeigt.

Weiter

Klicken Sie auf einen Desktop-Namen, um Einzelheiten zu diesem Desktop anzuzeigen, oder klicken Sie in View Administrator auf **[Back (Zurück)]** , um erneut auf die Dashboard-Seite zu wechseln.

Desktop-Status virtueller Maschinen

VM-Desktops, die von vCenter Server verwaltet werden, können verschiedene Betriebs- und Verfügbarkeitsstatus aufweisen. Der Status von Desktops wird in View Administrator auf der Seite mit der Desktop-Liste in der rechten Spalte angezeigt.

Tabelle 11-5 zeigt die Betriebsstatus von VM-Desktops, die in View Administrator angezeigt werden. Ein Desktop kann jeweils nur einen Status aufweisen.

Tabelle 11-5. Status von VM-Desktops, die über vCenter Server verwaltet werden

Status	Statustyp	Beschreibung
Bereitstellung	Bereitstellung	Die virtuelle Maschine wird gegenwärtig bereitgestellt.
Provisioning error (Bereitstellungsfehler)	Bereitstellung	Während der Bereitstellung ist ein Fehler aufgetreten.
Customizing (Wird angepasst)	Bereitstellung	Die virtuelle Maschine in einem automatisierten Pool wird angepasst.
Deleting (Wird gelöscht)	Bereitstellung	Die virtuelle Maschine ist für den Löschvorgang gekennzeichnet. Die virtuelle Maschine wird bald durch View Manager gelöscht.
Waiting for Agent (Warten auf Agent)	Agent-Status	View Connection Server wartet auf die Kommunikation mit View Agent in einer virtuellen Maschine in einem manuellen Pool. **Hinweis** Dieser Status entspricht dem Anpassungsstatus für eine virtuelle Maschine in einem automatisierten Pool.
Startup (Start)	Agent-Status	View Agent wurde auf der virtuellen Maschine gestartet, andere erforderliche Dienste (z.B. das Anzeigeprotokoll) werden jedoch gegenwärtig noch gestartet. View Agent kann beispielsweise erst eine RDP-Verbindung mit Clientcomputern herstellen, wenn der RDP-Startvorgang abgeschlossen wurde.
Agent unreachable (Agent nicht erreichbar)	Agent-Status	View Connection Server kann nicht mit View Agent in einer virtuellen Maschine kommunizieren.
Configuration error (Konfigurationsfehler)	Agent-Status	Das Anzeigeprotokoll, z.B. RDP oder PCoIP, ist nicht aktiviert.
Provisioned (Bereitgestellt)	Verfügbarkeit	Die virtuelle Maschine ist ausgeschaltet oder wurde angehalten.
Available (Verfügbar)	Verfügbarkeit	Die virtuelle Maschine ist eingeschaltet und kann für eine aktive Verbindung verwendet werden. In einem dedizierten Pool wird die virtuelle Maschine einem Benutzer zugewiesen und bei der Anmeldung des Benutzers gestartet.
Checked out (Ausgecheckt)	Sitzungsstatus	Die virtuelle Maschine für einen lokalen Desktop ist ausgecheckt.
Connected (Verbunden)	Sitzungsstatus	Die virtuelle Maschine befindet sich in einer aktiven Sitzung und verfügt über eine aktive Remote-Verbindung zu einer View Client-Instanz.
Disconnected (Getrennt)	Sitzungsstatus	Die virtuelle Maschine befindet sich in einer aktiven Sitzung, ist jedoch von der View Client-Instanz getrennt.
Unassigned user connected (Nicht zugewiesener Benutzer verbunden)	Miscellaneous (Sonstiges)	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist an einer virtuellen Maschine in einem dedizierten Pool angemeldet. Dieser Status kann beispielsweise auftreten, wenn ein Administrator vSphere Client startet, eine Konsole in der virtuellen Maschine öffnet und sich anmeldet.
Unassigned user disconnected (Nicht zugewiesener Benutzer getrennt)	Miscellaneous (Sonstiges)	Ein Benutzer, bei dem es sich nicht um den zugewiesenen Benutzer handelt, ist angemeldet und von einer virtuellen Maschine in einem dedizierten Pool getrennt.

Tabelle 11-5. Status von VM-Desktops, die über vCenter Server verwaltet werden (Fortsetzung)

Status	Statustyp	Beschreibung
Unknown (Unbekannt)	Miscellaneous (Sonstiges)	Die virtuelle Maschine weist einen unbekannten Status auf.
Maintenance mode (Wartungsmodus)	Miscellaneous (Sonstiges)	Die virtuelle Maschine befindet sich im Wartungsmodus. Benutzer können sich nicht an der virtuellen Maschine anmelden oder diese verwenden.
Error (Fehler)	Miscellaneous (Sonstiges)	In der virtuellen Maschine ist ein unbekannter Fehler aufgetreten.
–	Miscellaneous (Sonstiges)	Während die virtuelle Maschine einen der vorherigen Status aufwies, ist ein Fehler aufgetreten.

Wenn ein Desktop einen bestimmten Status aufweist, können weitere Bedingungen gelten. View Administrator zeigt diese Bedingungen als Suffixe des Desktop-Status an. Ein möglicher Status in View Administrator ist z.B. `Customizing (missing) (Wird angepasst (fehlt))`.

Tabelle 11-6 zeigt diese zusätzlichen Bedingungen.

Tabelle 11-6. Desktop-Status-Bedingungen

Bedingung	Beschreibung
Missing (Fehlt)	Die virtuelle Maschine ist in vCenter Server nicht vorhanden. Typischerweise wurde die virtuelle Maschine in vCenter Server gelöscht, in der View LDAP-Konfiguration ist jedoch noch ein Eintrag für den Desktop vorhanden.
Task halted (Aufgabe angehalten)	Ein View Composer-Vorgang, z.B. eine Aktualisierung, Neuzusammenstellung oder Neuverteilung, wurde angehalten. Weitere Informationen zur Fehlerbehebung bei Neuzusammenstellungen finden Sie unter „Korrigieren einer nicht erfolgreichen Neuzusammenstellung“, auf Seite 238. Weitere Informationen zu View Composer-Fehlerstatus finden Sie unter „View Composer-Bereitstellungsfehler“, auf Seite 376. Die Bedingung `Task halted (Aufgabe angehalten)` gilt für alle virtuellen Maschinen, die für den Vorgang ausgewählt wurden, für die der Vorgang jedoch noch nicht gestartet wurde. Auf virtuelle Maschinen innerhalb des Pools, die nicht für den Vorgang ausgewählt wurden, wird die Bedingung `Task halted (Aufgabe angehalten)` nicht angewendet.

Ein Desktop-Status kann beide Bedingungen aufweisen `(missing, task halted) (fehlt, Aufgabe angehalten)`, wenn eine View Composer-Aufgabe angehalten wurde und die virtuelle Maschine nicht in vCenter Server vorhanden ist.

Löschen von Desktops aus View Manager

Wenn Sie Desktops aus View Manager löschen, können die Benutzer nicht länger auf die Desktops zugreifen.

Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, können Benutzer mit derzeit aktiven Sitzungen Desktops auf Grundlage vollständiger virtueller Maschinen weiterhin verwenden. Nach der Abmeldung der Benutzer können diese nicht länger auf die gelöschten Desktops zugreifen.

Bei Linked-Clone-Desktops löscht vCenter Server die virtuellen Maschinen immer von der Festplatte.

Hinweis Löschen Sie die virtuellen Maschinen in vCenter Server erst, wenn Sie die Desktops mit View Administrator gelöscht haben. Anderenfalls könnte dies dazu führen, dass die View-Komponenten einen inkonsistenten Status aufweisen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Desktops]** .

2 Wählen Sie einen oder mehrere Desktops aus und klicken Sie auf **[Remove (Entfernen)]** .

3 Wählen Sie, wie die Desktops gelöscht werden sollen.

Option	Beschreibung
Pool that contains full virtual-machine desktops (Pool mit Desktops auf Grundlage vollständiger virtueller Maschinen)	Legen Sie fest, ob die virtuellen Maschinen in vCenter Server beibehalten oder gelöscht werden sollen. Wenn Sie die virtuellen Maschinen von der Festplatte löschen, werden Benutzer mit aktiven Sitzungen von ihren Desktops getrennt. Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, legen Sie fest, ob Benutzer mit aktiven Sitzungen mit ihren Desktops verbunden bleiben oder getrennt werden sollen.
Linked-clone pool with View Composer persistent disks (Linked-Clone-Pool mit persistenten View Composer-Festplatten)	Legen Sie fest, ob die persistenten Festplatten nach dem Löschen des Desktops getrennt oder gelöscht werden sollen. In beiden Fällen löscht vCenter Server die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit gegenwärtig aktiven Sitzungen werden von ihren Linked-Clone-Desktops getrennt. Wenn Sie eine persistente Festplatte trennen, kann sie mit einem anderen Desktop verknüpft werden. Getrennte persistente Festplatten können in demselben Datenspeicher oder in einem anderen Datenspeicher platziert werden.
Linked-clone pool without View Composer persistent disks (Linked-Clone-Pool ohne persistente View Composer-Festplatten)	vCenter Server löscht die virtuellen Linked-Clone-Maschinen von der Festplatte. Benutzer mit gegenwärtig aktiven Sitzungen werden von ihren Linked-Clone-Desktops getrennt.

Die Desktops werden aus View Connection Server entfernt. Wenn Sie die virtuellen Maschinen in vCenter Server beibehalten, kann View Manager nicht darauf zugreifen.

Beim Löschen von Desktops aus View Manager werden Linked-Clone-Computerkonten aus Active Directory entfernt. Die Konten vollständiger virtueller Maschinen sind weiterhin in Active Directory vorhanden. Diese Konten müssen manuell aus Active Directory entfernt werden.

Beim Löschen lokaler Desktops werden die Rechenzentrumskopien der Desktops aus View Manager entfernt. Die lokalen Desktops sind nicht mehr funktionsfähig, wenn die Clients View Connection Server kontaktieren oder die maximale Dauer ohne Serverkontakt überschritten wird. Wenn Sie festlegen, dass vollständige virtuelle Maschinen in vCenter Server beibehalten werden, oder wenn Sie persistente View Composer-Festplatten trennen und speichern, werden Benutzeränderungen an lokalen Desktops seit der letzten Replikation oder seit dem letzten Auschecken nicht auf den virtuellen Maschinen oder persistenten Festplatten beibehalten.

Exportieren von View-Informationen in externe Dateien

In View Administrator können View-Tabelleninformationen in externe Dateien exportiert werden. Sie können die Tabellen mit Benutzern und Gruppen, Pools, Desktops, persistenten View Composer-Festplatten, ThinApp-Anwendungen, Ereignissen und VDI-Sitzungen exportieren. Anschließend können diese Informationen in einer Kalkulationstabelle oder in einem anderen Tool angezeigt und verwaltet werden.

Sie können beispielsweise Informationen zu Desktops erfassen, die von mehreren View Connection Server-Instanzen oder Gruppen aus replizierten View Connection Server-Instanzen verwaltet werden. Die Tabelle **[Desktops]** kann über jede View Administrator-Schnittstelle exportiert und in einer Tabellenkalkulation angezeigt werden.

Beim Export einer View Administrator-Tabelle wird diese als kommagetrennte `.cvs`-Datei gespeichert. Über diese Funktion werden nicht einzelne Seiten, sondern die gesamte Tabelle exportiert.

Vorgehensweise

1 Zeigen Sie die zu exportierende Tabelle in View Administrator an.

Klicken Sie beispielsweise auf **[Inventory (Bestandsliste)] > [Desktops]** , um die Tabelle mit Desktops anzuzeigen.

2 Klicken Sie in der oberen rechten Ecke der Tabelle auf das Symbol **[Export (Exportieren)]** .

Wenn Sie mit dem Mauscursor auf das Symbol zeigen, wird die QuickInfo `Export table contents (Tabelleninhalte exportieren)` angezeigt.

3 Geben Sie im Dialogfeld **[Select location for download (Speicherort für Download auswählen)]** einen Dateinamen für die `.csv`-Datei ein.

Der standardmäßige Dateiname lautet `global_table_data_export.csv`.

4 Navigieren Sie zu einem Verzeichnis zum Speichern der Datei.

5 Klicken Sie auf **[Save (Speichern)]** .

Weiter

Öffnen Sie eine Tabellenkalkulation oder ein anderes Tool, um die `.csv`-Datei anzuzeigen.

Verwalten von physischen Computern und Terminalservern 12

Sie können in View Administrator View-Desktops, die nicht von vCenter Server verwaltet werden, hinzufügen, entfernen oder die Registrierung für diese Desktops aufheben. Nicht verwaltete Desktop-Quellen umfassen virtuelle Maschinen, physische Computer, Blade-PCs und Microsoft-Terminaldienste-Quellen, die nicht von vCenter Server verwaltet werden.

Hinweis Beim Neukonfigurieren einer Einstellung, die sich auf eine nicht verwaltete Desktop-Quelle auswirkt, wird die neue Einstellung möglicherweise erst nach bis zu 10 Minuten übernommen. Wenn Sie z.B. den Sicherheitsmodus für Nachrichten in den globalen Einstellungen oder die Einstellung zur automatischen Abmeldung nach der Verbindungstrennung für einen Pool ändern, kann es bis zu 10 Minuten dauern, bis View Manager die betroffenen nicht verwalteten Desktop-Quellen neu konfiguriert.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen einer nicht verwalteten Desktop-Quelle zu einem Pool“, auf Seite 263
- „Entfernen einer nicht verwalteten Desktop-Quelle aus einem Pool“, auf Seite 264
- „Löschen eines Pools mit nicht verwalteten Desktops“, auf Seite 264
- „Aufheben der Registrierung für eine nicht verwaltete Desktop-Quelle“, auf Seite 265
- „Desktop-Status von physischen Computern und Terminalservern“, auf Seite 265

Hinzufügen einer nicht verwalteten Desktop-Quelle zu einem Pool

Die Größe eines manuellen Desktop-Pools mit nicht verwalteten Desktop-Quellen kann erhöht werden, indem Desktop-Quellen zum Pool hinzugefügt werden.

Voraussetzungen

Stellen Sie sicher, dass View Agent auf der nicht verwalteten Desktop-Quelle installiert ist. Siehe „Installieren von View Agent auf einer nicht verwalteten Desktop-Quelle“, auf Seite 48.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Klicken Sie in der linken Spalte der Tabelle **[Pools]** auf die Pool-ID des manuellen Pools.

3 Klicken Sie auf der Registerkarte **[Inventory (Bestandsliste)]** auf **[Add (Hinzufügen)]** .

4 Wählen Sie im Fenster **[Add Desktops (Desktops hinzufügen)]** Desktop-Quellen aus und klicken Sie auf **[OK]** .

View Manager fügt die Desktop-Quelle zum Pool hinzu.

Entfernen einer nicht verwalteten Desktop-Quelle aus einem Pool

Die Größe eines manuellen Desktop-Pools mit nicht verwalteten Desktop-Quellen kann verringert werden, indem Desktop-Quellen aus dem Pool entfernt werden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Doppelklicken Sie auf eine Pool-ID und wählen Sie die Registerkarte **[Inventory (Bestandsliste)]** .

3 Wählen Sie die zu entfernenden Desktop-Quellen aus.

4 Klicken Sie auf **[Remove (Entfernen)]** .

5 Wenn Benutzer an den nicht verwalteten Desktops angemeldet sind, legen Sie fest, ob die Sitzungen beendet werden oder aktiv bleiben sollen.

Option	Beschreibung
Leave active (Aktiv lassen)	Aktive Sitzungen bleiben bestehen, bis der Benutzer sich abmeldet. View Connection Server verfolgt diese Sitzungen nicht nach.
Terminate (Beenden)	Aktive Sitzungen werden sofort beendet.

6 Klicken Sie auf **[OK]** .

View Manager entfernt die Desktop-Quellen aus dem Pool.

Löschen eines Pools mit nicht verwalteten Desktops

Wenn Sie einen Desktop-Pool mit nicht verwalteten Desktop-Quellen löschen, wird der Pool aus View Manager entfernt.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Inventory (Bestandsliste)]** > **[Pools]** .

2 Wählen Sie einen nicht verwalteten Desktop-Pool aus und klicken Sie auf **[Delete (Löschen)]** .

3 Wenn Benutzer an den nicht verwalteten Desktops angemeldet sind, legen Sie fest, ob die Sitzungen beendet werden oder aktiv bleiben sollen.

Option	Beschreibung
Leave active (Aktiv lassen)	Aktive Sitzungen bleiben bestehen, bis der Benutzer sich abmeldet. View Connection Server verfolgt diese Sitzungen nicht nach.
Terminate (Beenden)	Aktive Sitzungen werden sofort beendet.

4 Klicken Sie auf **[OK]** .

Der nicht verwaltete Desktop-Pool wird aus View Manager entfernt. Die Registrierungsinformationen für die nicht verwalteten Desktop-Quellen des Pools werden nicht entfernt.

Um die nicht verwalteten Desktop-Quellen aus View Manager zu entfernen, muss die Registrierung aufgehoben werden. Siehe „Aufheben der Registrierung für eine nicht verwaltete Desktop-Quelle“, auf Seite 265.

Aufheben der Registrierung für eine nicht verwaltete Desktop-Quelle

Alle von vCenter Server verwalteten Desktop-Quellen werden bei der Installation von View Agent registriert. Sie können nur die Registrierung nicht verwalteter Desktop-Quellen aufheben.

Nicht verwaltete Desktop-Quellen umfassen virtuelle Maschinen, physische Computer, Blade-PCs und Terminaldienstequellen, die nicht von vCenter Server verwaltet werden.

Wenn Sie die Registrierung einer Desktop-Quelle aufheben, steht diese nicht mehr in View Manager zur Verfügung. Um eine Quelle wieder verfügbar zu machen, installieren Sie View Agent in der Desktop-Quelle neu.

Voraussetzungen

Stellen Sie sicher, dass die Desktop-Quellen, deren Registrierung aufgehoben werden soll, nicht in Desktop-Pools verwendet werden.

Vorgehensweise

1 Klicken Sie auf **[View Configuration (View-Konfiguration)] > [Registered desktop sources (Registrierte Desktop-Quellen)]** .

2 Wählen Sie den Typ der nicht verwalteten Desktop-Quelle aus und klicken Sie auf **[Details]** .

3 Wählen Sie die Desktop-Quelle aus, deren Registrierung aufgehoben werden soll, und klicken Sie auf **[Unregister (Registrierung aufheben)]** .

   Sie können nur Desktop-Quellen auswählen, die nicht von einem Desktop-Pool verwendet werden.

4 Klicken Sie auf **[OK]** , um zu bestätigen, dass die Registrierung der Desktop-Quelle aufgehoben werden soll.

Die Registrierung der Desktop-Quelle wird aufgehoben, und die Quelle ist nicht länger verfügbar.

Desktop-Status von physischen Computern und Terminalservern

Desktop-Quellen, bei denen es sich um physische Computer, Terminalserver oder virtuelle Maschinen handelt, die nicht von vCenter Server verwaltet werden, können verschiedene Betriebs- und Verfügbarkeitsstatus aufweisen. Der Status von Desktops wird in View Administrator auf der Seite mit der Desktop-Liste in der rechten Spalte angezeigt.

Tabelle 12-1 zeigt die Betriebsstatus von physischen Computer- und Terminalserver-Desktops, die in View Administrator angezeigt werden. Ein Desktop kann jeweils nur einen Status aufweisen.

Tabelle 12-1. Status von Desktops, bei denen es sich um physische Computer oder Terminalserver handelt

Status	Statustyp	Beschreibung
Waiting for Agent (Warten auf Agent)	Agent-Status	View Connection Server wartet auf dem Empfang der ersten Anforderung von View Agent auf einem physischen Computer- oder Terminalserver-Desktop.
Agent not reachable (Agent nicht erreichbar)	Agent-Status	View Connection Server kann nicht mit View Agent auf dem Desktop kommunizieren. Der als Desktop-Quelle eingesetzte Computer ist möglicherweise ausgeschaltet.
Configuration error (Konfigurationsfehler)	Agent-Status	Das Anzeigeprotokoll (z.B. RDP), ein Terminalserver oder ein anderes Protokoll ist nicht aktiviert.
Available (Verfügbar)	Verfügbarkeit	Der als Desktop-Quelle eingesetzte Computer ist eingeschaltet und es kann eine aktive Verbindung mit dem Desktop hergestellt werden. In einem dedizierten Pool wird der Desktop einem Benutzer zugewiesen. Der Desktop wird bei der Anmeldung des Benutzers gestartet.

Tabelle 12-1. Status von Desktops, bei denen es sich um physische Computer oder Terminalserver handelt (Fortsetzung)

Status	Statustyp	Beschreibung
Connected (Verbunden)	Sitzungsstatus	Der Desktop befindet sich in einer aktiven Sitzung und verfügt über eine aktive Remote-Verbindung zu einer View Client-Instanz.
Disconnected (Getrennt)	Sitzungsstatus	Der Desktop befindet sich in einer aktiven Sitzung, ist jedoch von der View Client-Instanz getrennt.
–	Miscellaneous (Sonstiges)	Während der Desktop einen der vorherigen Status aufwies, ist ein Fehler aufgetreten.

Verwalten von ThinApp-Anwendungen in View Administrator 13

Sie können View Administrator zum Verteilen und Verwalten von Anwendungen verwenden, die mit VMware ThinApp™ verpackt wurden. Die Verwaltung von ThinApp-Anwendungen in View Administrator umfasst das Erfassen und Speichern von Anwendungspaketen, das Hinzufügen von ThinApp-Anwendungen zu View Administrator und das Zuweisen von ThinApp-Anwendungen zu Desktops und Pools.

Zur Verwendung der ThinApp-Verwaltungsfunktion in View Administrator benötigen Sie eine Lizenz.

Dieses Kapitel behandelt die folgenden Themen:

- „View-Anforderungen für ThinApp-Anwendungen“, auf Seite 267
- „Erfassen und Speichern von Anwendungspaketen“, auf Seite 268
- „Zuweisen von ThinApp-Anwendungen zu Desktops und Pools“, auf Seite 272
- „Warten von ThinApp-Anwendungen in View Administrator“, auf Seite 279
- „Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in View Administrator“, auf Seite 282
- „ThinApp-Konfigurationsbeispiel“, auf Seite 286

View-Anforderungen für ThinApp-Anwendungen

Beim Erfassen und Speichern von ThinApp-Anwendungen zur Verteilung an View-Desktops in View Administrator müssen bestimmte Anforderungen erfüllt werden.

- Sie müssen Ihre Anwendungen als MSI-Pakete (Microsoft Installation) paketieren.
- Zum Erstellen oder erneuten Paketieren der MSI-Pakete benötigen Sie ThinApp 4.6 oder höher.
- Speichern Sie die MSI-Pakete auf einer Windows-Netzwerkfreigabe, die sich in einer Active Directory-Domäne befindet, auf die Ihr View Connection Server-Host und View-Desktops zugreifen können. Der Dateiserver muss Authentifizierung und Dateiberechtigungen unterstützen, die auf Computerkonten basieren.
- Sie müssen die Datei- und Freigabeberechtigungen auf der Netzwerkfreigabe festlegen, auf der sich die MSI-Pakete befinden, um der integrierten Active Directory-Gruppe **[Domain Computers (Domänencomputer)]** Lesezugriff zu gewähren. Wenn Sie ThinApp-Anwendungen an Domänencontroller verteilen möchten, müssen Sie der integrierten Active Directory-Gruppe **[Domain Controllers (Domänencontroller)]** Lesezugriff gewähren.
- Wenn Sie das Streaming von ThinApp-Anwendungspaketen durch Benutzer zulassen möchten, müssen Sie die NTFS-Berechtigung der Netzwerkfreigabe, auf der die ThinApp-Pakete gehostet werden, auf `Read&Execute (Lesen &Ausführen)` festlegen.

- Stellen Sie sicher, dass ein nicht zusammenhängender Namespace Domänenmitgliedscomputer nicht daran hindert, auf die Netzwerkfreigabe zuzugreifen, auf der die MSI-Pakete gehostet werden. Ein nicht zusammenhängender Namespace liegt vor, wenn sich der Name einer Active Directory-Domäne vom DNS-Namespace unterscheidet, der von den Computern in dieser Domäne verwendet wird. Weitere Informationen finden Sie im VMware Knowledge Base-Artikel 1023309.
- Zur Ausführung gestreamter ThinApp-Anwendungen auf View-Desktops müssen Benutzer auf die Netzwerkfreigabe mit den MSI-Paketen zugreifen können.

Erfassen und Speichern von Anwendungspaketen

ThinApp ermöglicht die Anwendungsvirtualisierung, indem eine Anwendung von dem zugrunde liegenden Betriebssystem und dessen Bibliotheken und Framework entkoppelt und anschließend in eine ausführbare Datei gebündelt wird. Diese wird als Anwendungspaket bezeichnet.

Um ThinApp-Anwendungen in View Administrator zu verwalten, muss der ThinApp Setup Capture-Assistent zum Erfassen und Erstellen von Anwendungspaketen im MSI-Format sowie zum Speichern der MSI-Pakete in einem Anwendungs-Repository verwendet werden.

Bei einem Anwendungs-Repository handelt es sich um eine Windows-Netzwerkfreigabe. Die Netzwerkfreigabe wird über View Administrator als Anwendungs-Repository registriert. Sie können auch mehrere Anwendungs-Repositorys registrieren.

Hinweis Wenn Sie über mehrere Anwendungs-Repositorys verfügen, können Sie den Lastausgleich und die Verfügbarkeit mithilfe von Drittanbieterlösungen verwalten. View umfasst keine Lösungen für Lastausgleich oder Verfügbarkeit.

Vollständige Informationen zu ThinApp-Funktionen und zur Verwendung des ThinApp Setup Capture-Assistenten finden Sie in der *Einführung in VMware ThinApp* und im *ThinApp-Benutzerhandbuch*.

1 Paketieren von Anwendungen auf Seite 269

Verwenden Sie den ThinApp Setup Capture-Assistenten, um Ihre Anwendungen zu paketieren.

2 Erstellen einer Windows-Netzwerkfreigabe auf Seite 269

Zum Hosten der MSI-Pakete, die an View-Desktops und -Pools verteilt werden, müssen Sie in View Administrator eine Windows-Netzwerkfreigabe erstellen.

3 Registrieren eines Anwendungs-Repositorys auf Seite 270

Sie müssen die Windows-Netzwerkfreigabe registrieren, die als Anwendungs-Repository für Ihre MSI-Pakete in View Administrator verwendet wird.

4 Hinzufügen von ThinApp-Anwendungen zu View Administrator auf Seite 270

Sie fügen ThinApp-Anwendungen zu View Administrator hinzu, indem Sie ein Anwendungs-Repository durchsuchen und ThinApp-Anwendungen auswählen. Nach dem Hinzufügen einer ThinApp-Anwendung zu View Administrator kann die Anwendung Desktops oder Pools zugewiesen werden.

5 Erstellen einer ThinApp-Vorlage auf Seite 271

Sie können in View Administrator eine Vorlage erstellen, um eine Gruppe aus ThinApp-Anwendungen anzugeben. Mithilfe von Vorlagen können Sie Anwendungen nach Funktion, Anbieter oder einer beliebigen anderen logischen Gruppierung zusammenfassen, die in Ihrer Organisation sinnvoll ist.

Paketieren von Anwendungen

Verwenden Sie den ThinApp Setup Capture-Assistenten, um Ihre Anwendungen zu paketieren.

Voraussetzungen

- Laden Sie die ThinApp-Software von der Seite http://www.vmware.com/de/products/thinapp herunter und installieren Sie sie auf einem Computer, auf dem noch keine Version dieser Software vorhanden ist. View unterstützt ThinApp 4.6 und höher.
- Machen Sie sich mit den ThinApp-Softwareanforderungen und den Anweisungen zur Paketerstellung im *ThinApp-Benutzerhandbuch* vertraut.

Vorgehensweise

1. Starten Sie den ThinApp Setup Capture-Assistenten und folgen Sie dessen Anweisungen.
2. Wenn Sie der ThinApp Setup Capture-Assistent auffordert, einen Projektspeicherort anzugeben, wählen Sie **[Build MSI package (MSI-Paket erstellen)]** .
3. Wenn Sie ein Streaming der Anwendung auf View-Desktops planen, legen Sie die MSIStreaming-Eigenschaft in der Datei `package.ini` auf den Wert 1 fest.

```
MSIStreaming=1
```

Der ThinApp Setup Capture-Assistent kapselt die Anwendung, alle zum Ausführen der Anwendung erforderlichen Komponenten und die Anwendung selbst in einem MSI-Paket.

Weiter

Erstellen Sie zum Speichern der MSI-Pakete eine Windows-Netzwerkfreigabe.

Erstellen einer Windows-Netzwerkfreigabe

Zum Hosten der MSI-Pakete, die an View-Desktops und -Pools verteilt werden, müssen Sie in View Administrator eine Windows-Netzwerkfreigabe erstellen.

Voraussetzungen

- Verwenden Sie den ThinApp Capture Setup-Assistenten, um die Anwendungen zu paketieren.
- Stellen Sie sicher, dass die Netzwerkfreigabe die View-Anforderungen zum Speichern von ThinApp-Anwendungen erfüllt. Weitere Informationen finden Sie unter „View-Anforderungen für ThinApp-Anwendungen“, auf Seite 267.

Vorgehensweise

1. Erstellen Sie eine Ordnerfreigabe auf einem Computer in einer Active Directory-Domäne, auf die Ihr View Connection Server-Host und View-Desktops zugreifen können.
2. Konfigurieren Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe **[Domain Computers (Domänencomputer)]** Lesezugriff zu gewähren.
3. Wenn Sie Domänencontrollern ThinApp-Anwendungen zuweisen möchten, müssen Sie der integrierten Active Directory-Gruppe **[Domain Controllers (Domänencontroller)]** Lesezugriff gewähren.
4. Wenn Sie das Streaming von ThinApp-Anwendungspaketen planen, legen Sie die NTFS-Berechtigung der Netzwerkfreigabe, auf der die ThinApp-Pakete gehostet werden, auf `Read&Execute (Lesen &Ausführen)` für die Benutzer fest.
5. Kopieren Sie die MSI-Pakete in den freigegebenen Ordner.

Weiter

Registrieren Sie die Windows-Netzwerkfreigabe als Anwendungs-Repository in View Administrator.

Registrieren eines Anwendungs-Repositorys

Sie müssen die Windows-Netzwerkfreigabe registrieren, die als Anwendungs-Repository für Ihre MSI-Pakete in View Administrator verwendet wird.

Sie können auch mehrere Anwendungs-Repositorys registrieren.

Voraussetzungen

Erstellen Sie eine Windows-Netzwerkfreigabe.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [ThinApp Configuration (ThinApp-Konfiguration)]** und klicken Sie auf **[Add Repository (Repository hinzufügen)]** .

2 Geben Sie in das Textfeld **[Display name (Anzeigename)]** einen Anzeigenamen für das Anwendungs-Repository ein.

3 Geben Sie in das Textfeld **[Share path (Freigabepfad)]** den Pfad zur Windows-Netzwerkfreigabe mit Ihren Anwendungspaketen ein.

   Der Pfad zur Netzwerkfreigabe muss in der Form *Computername_des_Servers**Freigabename* angegeben werden, wobei *Computername_des_Servers* den DNS-Namen des Servercomputers angibt. Geben Sie keine IP-Adresse an.

   Beispiel: `\\Server.Domaene.com\MSIPackages`

4 Klicken Sie auf **[Save (Speichern)]** , um das Anwendungs-Repository in View Administrator zu registrieren.

Hinzufügen von ThinApp-Anwendungen zu View Administrator

Sie fügen ThinApp-Anwendungen zu View Administrator hinzu, indem Sie ein Anwendungs-Repository durchsuchen und ThinApp-Anwendungen auswählen. Nach dem Hinzufügen einer ThinApp-Anwendung zu View Administrator kann die Anwendung Desktops oder Pools zugewiesen werden.

Voraussetzungen

Registrieren Sie ein Anwendungs-Repository mit View Administrator.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** .

2 Klicken Sie auf der Registerkarte **[Summary (Übersicht)]** auf **[Scan New ThinApps (Neue ThinApps durchsuchen)]** .

3 Wählen Sie ein Anwendungs-Repository und einen Ordner für die Suche aus und klicken Sie auf **[Next (Weiter)]** .

   Wenn das Anwendungs-Repository Unterordner enthält, können Sie den Stammordner erweitern und einen Unterordner auswählen.

4 Wählen Sie die ThinApp-Anwendungen, die zu View Administrator hinzugefügt werden sollen.

   Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere ThinApp-Anwendungen auszuwählen.

5 Klicken Sie auf **[Scan (Durchsuchen)]** , um die ausgewählten MSI-Pakete zu durchsuchen.

Wenn die Suche angehalten werden muss, klicken Sie auf **[Stop Scan (Suche beenden)]** .

View Administrator zeigt den Status der einzelnen Suchvorgänge und die Anzahl an ThinApp-Anwendungen an, die zu View Administrator hinzugefügt wurden. Bei Auswahl einer Anwendung, die sich bereits in View Administrator befindet, wird diese nicht erneut hinzugefügt.

6 Klicken Sie auf **[Finish (Fertig stellen)]** .

Die neuen ThinApp-Anwendungen werden auf der Registerkarte **[Summary (Übersicht)]** angezeigt.

Weiter

(Optional) Erstellen Sie ThinApp-Vorlagen.

Erstellen einer ThinApp-Vorlage

Sie können in View Administrator eine Vorlage erstellen, um eine Gruppe aus ThinApp-Anwendungen anzugeben. Mithilfe von Vorlagen können Sie Anwendungen nach Funktion, Anbieter oder einer beliebigen anderen logischen Gruppierung zusammenfassen, die in Ihrer Organisation sinnvoll ist.

Mit ThinApp-Vorlagen lässt sich die Verteilung mehrerer Anwendungen optimieren. Wenn Sie einem Desktop oder Pool eine ThinApp-Vorlage zuweisen, installiert View Administrator alle gegenwärtig in der Vorlage enthaltenen Anwendungen.

Das Erstellen von ThinApp-Vorlagen ist optional.

Hinweis Wenn Sie eine Anwendung zu einer ThinApp-Vorlage hinzufügen, nachdem die Vorlage einem Desktop oder Pool zugewiesen wurde, weist View Administrator die neue Anwendung nicht automatisch dem Desktop oder Pool zu. Beim Entfernen einer Anwendung aus einer ThinApp-Vorlage, die zuvor einem Desktop oder Pool zugewiesen wurde, wird die Zuweisung der Anwendung zum Desktop oder Pool beibehalten.

Voraussetzungen

Fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** . Klicken Sie anschließend auf **[New Template (Neue Vorlage)]** .

2 Geben Sie den Namen der Vorlage ein und klicken Sie auf **[Add (Hinzufügen)]** .

Alle verfügbaren ThinApp-Anwendungen werden in der Tabelle angezeigt.

3 Um nach einer bestimmten ThinApp-Anwendung zu suchen, geben Sie den Namen der Anwendung in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

4 Wählen Sie die ThinApp-Anwendungen aus, die in die Vorlage aufgenommen werden sollen, und klicken Sie auf **[Add (Hinzufügen)]** .

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Anwendungen auszuwählen.

5 Klicken Sie auf **[OK]** , um die Vorlage zu speichern.

Zuweisen von ThinApp-Anwendungen zu Desktops und Pools

Um eine ThinApp-Anwendung auf einem View-Desktop zu installieren, weisen Sie die ThinApp-Anwendung über View Administrator einem Desktop oder Pool zu.

Wenn Sie einem Desktop eine ThinApp-Anwendung zuweisen, beginnt View Administrator wenige Minuten später mit der Installation der Anwendung auf dem Desktop. Wenn Sie einem Pool eine ThinApp-Anwendung zuweisen, beginnt View Administrator mit der Installation der Anwendung, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet.

Streaming	View Administrator installiert eine Verknüpfung mit der ThinApp-Anwendung auf dem Desktop. Die Verknüpfung weist auf die ThinApp-Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung gestreamter ThinApp-Anwendungen müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	View Administrator installiert die vollständige ThinApp-Anwendung auf dem lokalen Dateisystem.

Die Installationsdauer einer ThinApp-Anwendung hängt von der Größe der Anwendung ab.

Wichtig Sie können ThinApp-Anwendungen zu Desktops und Pools zuweisen, die nur über virtuelle Maschinen als Quellen verfügen. Das Zuweisen von ThinApp-Anwendungen zu Terminalservern, Blade-PCs oder herkömmlichen PCs ist nicht möglich.

- Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen auf Seite 273

  Befolgen Sie beim Zuweisen von ThinApp-Anwendungen zu Desktops und Pools die empfohlenen Vorgehensweisen.

- Zuweisen einer ThinApp-Anwendung zu mehreren Desktops auf Seite 273

  Sie können einem oder mehreren Desktops eine bestimmte ThinApp zuweisen.

- Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop auf Seite 274

  Sie können einem bestimmten Desktop eine oder mehrere ThinApp-Anwendungen zuweisen.

- Zuweisen einer ThinApp-Anwendung zu mehreren Pools auf Seite 275

  Sie können einem oder mehreren Pools eine bestimmte ThinApp-Anwendung zuweisen.

- Zuweisen mehrerer ThinApp-Anwendungen zu einem Pool auf Seite 276

  Sie können einem bestimmten Pool eine oder mehrere ThinApp-Anwendungen zuweisen.

- Zuweisen einer ThinApp-Vorlage zu einem Desktop oder Pool auf Seite 276

  Um die Verteilung mehrerer ThinApp-Anwendungen zu optimieren, können Sie einem Desktop oder Pool eine ThinApp-Vorlage zuweisen.

- Anzeigen von ThinApp-Anwendungszuweisungen auf Seite 277

  Sie können alle Desktops und Pools anzeigen, denen eine bestimmte ThinApp-Anwendung gegenwärtig zugewiesen ist. Sie können ebenso alle ThinApp-Anwendungen anzeigen, die einem bestimmten Desktop oder Pool zugewiesen sind.

- Anzeigen von MSI-Paketinformationen auf Seite 279

  Nach dem Hinzufügen einer ThinApp-Anwendung zu View Administrator können Sie Informationen zu den MSI-Paketen anzeigen.

Empfohlene Vorgehensweisen für die Zuweisung von ThinApp-Anwendungen

Befolgen Sie beim Zuweisen von ThinApp-Anwendungen zu Desktops und Pools die empfohlenen Vorgehensweisen.

- Zur Installation einer ThinApp-Anwendung auf einem bestimmten Desktop weisen Sie die Anwendung dem Desktop zu. Wenn Sie eine allgemeine Benennungskonvention für Ihre Desktops verwenden, können Sie Anwendungen mithilfe von Desktop-Zuweisungen schnell auf alle Desktops mit derselben Benennungskonvention verteilen.
- Um eine ThinApp-Anwendung auf allen Desktops innerhalb eines Pools zu installieren, weisen Sie die Anwendung dem Pool zu. Wenn Sie Pools nach Abteilung oder Benutzertyp organisieren, können Sie Anwendungen mithilfe von Pool-Zuweisungen schnell an bestimmte Abteilungen oder Benutzer verteilen. Wenn Sie beispielsweise über einen Pool für Benutzer in der Buchhaltungsabteilung verfügen, können Sie dieselbe Anwendung an alle Benutzer in der Buchhaltungsabteilung verteilen, indem Sie dem Buchhaltungs-Pool eine Anwendung zuweisen.
- Zum Optimieren der Verteilung mehrerer ThinApp-Anwendungen nehmen Sie die Anwendungen in eine ThinApp-Vorlage auf. Wenn Sie einem Desktop oder Pool eine ThinApp-Vorlage zuweisen, installiert View Administrator alle gegenwärtig in der Vorlage enthaltenen Anwendungen.
- Weisen Sie einem Desktop oder Pool keine ThinApp-Vorlagen mit ThinApp-Anwendungen zu, die dem Desktop oder Pool bereits zugewiesen sind. Weisen Sie einem Desktop oder Pool eine ThinApp-Vorlage ferner nicht mehrfach mit unterschiedlichem Installationstyp zu. View Administrator gibt in beiden Fällen ThinApp-Zuweisungsfehler zurück.
- Wenngleich die Zuweisung von ThinApp-Anwendungen zu lokalen Desktops nicht unterstützt wird, wird diese Vorgehensweise in View Administrator nicht verhindert. Wenn Sie ein wenig experimentieren und ThinApp-Anwendungen zu lokalen Desktops hinzufügen möchten, müssen jedoch bestimmte Anforderungen erfüllt sein. Wenn Sie vorhaben, eine ThinApp-Anwendung zu streamen, stellen Sie sicher, dass View Agent auf dem Desktop im lokalen Modus auf die Netzwerkfreigabe zugreifen kann, die das ThinApp-Repository hostet. Gestreamte ThinApp-Anwendungen funktionieren nur dann, wenn das Clientsystem mit dem Netzwerk verbunden ist.

  Das Zuweisen von ThinApp-Anwendungen und deren Entfernen von einem Desktop funktionieren nur dann, wenn sowohl der View Connection Server als auch der View Agent auf dem Desktop im lokalen Modus Zugriff auf die Netzwerkfreigabe haben, die das ThinApp-Repository hostet.

Vorsicht Ein Rollback eines Desktops kann dazu führen, dass View Connection Server nicht die richtigen Informationen zu den ThinApps auf diesem Desktop vorliegen.

Zuweisen einer ThinApp-Anwendung zu mehreren Desktops

Sie können einem oder mehreren Desktops eine bestimmte ThinApp zuweisen.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe „Hinzufügen von ThinApp-Anwendungen zu View Administrator“, auf Seite 270.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)] > [ThinApps]** und wählen Sie die ThinApp-Anwendung aus.

2 Wählen Sie im Dropdown-Menü **[Add Assignment (Zuweisung hinzufügen)]** die Option **[Desktops]** .

Die Desktops, denen die ThinApp-Anwendung noch nicht zugewiesen ist, werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einem bestimmten Desktop	Geben Sie den Namen des Desktops in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .
Suchen nach allen Desktops mit derselben Benennungskonvention	Geben Sie einen Teil des Desktop-Namens in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

3 Wählen Sie die Desktops aus, denen die ThinApp-Anwendung zugewiesen werden soll, und klicken Sie auf **[Add (Hinzufügen)]** .

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Desktops auszuwählen.

4 Wählen Sie einen Installationstyp und klicken Sie auf **[OK]** .

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

View Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendung. Nach der Installation steht die Anwendung allen Benutzern der Desktops zur Verfügung.

Zuweisen mehrerer ThinApp-Anwendungen zu einem Desktop

Sie können einem bestimmten Desktop eine oder mehrere ThinApp-Anwendungen zuweisen.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe „Hinzufügen von ThinApp-Anwendungen zu View Administrator“, auf Seite 270.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)]** > **[Desktops]** . Doppelklicken Sie anschließend in der Spalte **[Desktop]** auf den Namen des Desktops.

2 Klicken Sie auf der Registerkarte **[Summary (Übersicht)]** im ThinApps-Bereich auf **[Add Assignment (Zuweisung hinzufügen)]** .

Die ThinApp-Anwendungen, die dem Desktop noch nicht zugewiesen sind, werden in der Tabelle angezeigt.

3 Um nach einer bestimmten Anwendung zu suchen, geben Sie den Namen der Anwendung in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

4 Wählen Sie eine ThinApp-Anwendung aus, die dem Desktop zugewiesen werden soll, und klicken Sie auf **[Add (Hinzufügen)]** .

Wiederholen Sie diesen Schritt, um mehrere Anwendungen hinzuzufügen.

5 Wählen Sie einen Installationstyp und klicken Sie auf **[OK]** .

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

View Administrator beginnt wenige Minuten später mit der Installation der ThinApp-Anwendungen. Nach der Installation stehen die Anwendungen allen Benutzern des Desktops zur Verfügung.

Zuweisen einer ThinApp-Anwendung zu mehreren Pools

Sie können einem oder mehreren Pools eine bestimmte ThinApp-Anwendung zuweisen.

Wenn Sie einem Linked-Clone-Pool eine ThinApp-Anwendung zuweisen und den Pool zu einem späteren Zeitpunkt aktualisieren, neu zusammenstellen oder neu verteilen, installiert View Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe „Hinzufügen von ThinApp-Anwendungen zu View Administrator“, auf Seite 270.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)]** > **[ThinApps]** und wählen Sie die ThinApp-Anwendung aus.

2 Wählen Sie im Dropdown-Menü **[Add Assignment (Zuweisung hinzufügen)]** die Option **[Pools]** .

Die Pools, denen die ThinApp-Anwendung noch nicht zugewiesen ist, werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einem bestimmten Pool	Geben Sie den Namen des Pools in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .
Suchen nach allen Pools mit derselben Benennungskonvention	Geben Sie einen Teil des Pool-Namens in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

3 Wählen Sie die Pools aus, denen die ThinApp-Anwendung zugewiesen werden soll, und klicken Sie auf **[Add (Hinzufügen)]** .

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Pools auszuwählen.

4 Wählen Sie einen Installationstyp und klicken Sie auf **[OK]** .

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

View Administrator beginnt mit der Installation der ThinApp-Anwendung, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet. Nach der Installation steht die Anwendung allen Benutzern des Desktops zur Verfügung.

Zuweisen mehrerer ThinApp-Anwendungen zu einem Pool

Sie können einem bestimmten Pool eine oder mehrere ThinApp-Anwendungen zuweisen.

Wenn Sie einem Linked-Clone-Pool eine ThinApp-Anwendung zuweisen und den Pool zu einem späteren Zeitpunkt aktualisieren, neu zusammenstellen oder neu verteilen, installiert View Administrator die Anwendung erneut. Eine manuelle Neuinstallation der Anwendung ist nicht erforderlich.

Voraussetzungen

Durchsuchen Sie ein Anwendungs-Repository und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu. Siehe „Hinzufügen von ThinApp-Anwendungen zu View Administrator“, auf Seite 270.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)]** > **[Pools]** und doppelklicken Sie auf die Pool-ID.

2 Klicken Sie auf der Registerkarte **[Inventory (Bestandsliste)]** auf **[ThinApps]** und anschließend auf **[Add Assignment (Zuweisung hinzufügen)]** .

Die ThinApp-Anwendungen, die dem Pool noch nicht zugewiesen sind, werden in der Tabelle angezeigt.

3 Um nach einer bestimmten Anwendung zu suchen, geben Sie den Namen der ThinApp-Anwendung in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

4 Wählen Sie eine ThinApp-Anwendung aus, die dem Pool zugewiesen werden soll, und klicken Sie auf **[Add (Hinzufügen)]** .

Wiederholen Sie diesen Schritt, um mehrere Anwendungen auszuwählen.

5 Wählen Sie einen Installationstyp und klicken Sie auf **[OK]** .

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

View Administrator beginnt mit der Installation der ThinApp-Anwendungen, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet. Nach der Installation stehen die Anwendungen allen Benutzern des Desktops zur Verfügung.

Zuweisen einer ThinApp-Vorlage zu einem Desktop oder Pool

Um die Verteilung mehrerer ThinApp-Anwendungen zu optimieren, können Sie einem Desktop oder Pool eine ThinApp-Vorlage zuweisen.

Wenn Sie einem Desktop oder Pool eine ThinApp-Vorlage zuweisen, installiert View Administrator die gegenwärtig in der Vorlage enthaltenen ThinApp-Anwendungen.

Voraussetzungen

Erstellen Sie eine ThinApp-Vorlage. Siehe „Erstellen einer ThinApp-Vorlage“, auf Seite 271.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[ThinApps]** .

2 Wählen Sie die ThinApp-Vorlage.

3 Wählen Sie im Dropdown-Menü **[Add Assignment (Zuweisung hinzufügen)]** die Option **[Desktops]** oder **[Pools]** .

Sämtliche Desktops oder Pools werden in der Tabelle angezeigt.

Option	Aktion
Suchen nach einem bestimmten Desktop oder Pool	Geben Sie den Namen des Desktops oder Pools in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .
Suchen nach allen Desktops oder Pools mit derselben Benennungskonvention	Geben Sie einen Teil des Desktop- oder Pool-Namens in das Textfeld **[Find (Suchen)]** ein und klicken Sie auf **[Find (Suchen)]** .

4 Wählen Sie die Desktops oder Pools aus, denen die ThinApp-Vorlage zugewiesen werden soll, und klicken Sie auf **[Add (Hinzufügen)]** .

Wiederholen Sie diesen Schritt, um mehrere Desktops oder Pools auszuwählen.

5 Wählen Sie einen Installationstyp und klicken Sie auf **[OK]** .

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

Einige ThinApp-Anwendungen bieten keine Unterstützung für beide Installationstypen. Die Art und Weise, wie das Anwendungspaket erstellt wurde, bestimmt die verfügbaren Installationstypen.

Wenn Sie einem Desktop eine ThinApp-Vorlage zuweisen, beginnt View Administrator wenige Minuten später mit der Installation der in der Vorlage enthaltenen Anwendungen. Wenn Sie einem Pool eine ThinApp-Vorlage zuweisen, beginnt View Administrator mit der Installation der in der Vorlage enthaltenen Anwendungen, sobald sich ein Benutzer erstmalig an einem Desktop im Pool anmeldet. Nach der Installation stehen die Anwendungen allen Benutzern des Desktops bzw. Pools zur Verfügung.

Wenn eine ThinApp-Vorlage eine Anwendung enthält, die dem Desktop oder Pool bereits zugewiesen ist, gibt View Administrator einen Zuweisungsfehler für die Anwendung zurück.

Anzeigen von ThinApp-Anwendungszuweisungen

Sie können alle Desktops und Pools anzeigen, denen eine bestimmte ThinApp-Anwendung gegenwärtig zugewiesen ist. Sie können ebenso alle ThinApp-Anwendungen anzeigen, die einem bestimmten Desktop oder Pool zugewiesen sind.

Voraussetzungen

Machen Sie sich mit den verschiedenen ThinApp-Installationsstatuswerten unter „Installationsstatuswerte für ThinApp-Anwendungen“, auf Seite 278 vertraut.

Vorgehensweise

- Wählen Sie die ThinApp-Anwendungszuweisungen, die Sie anzeigen möchten.

Option	Aktion
Anzeigen aller Desktops und Pools, denen eine bestimmte ThinApp-Anwendung gegenwärtig zugewiesen ist	Wählen Sie **[Inventory (Bestandsliste)]** > **[ThinApps]** und doppelklicken Sie auf den Namen der ThinApp-Anwendung. Auf der Registerkarte **[Assignments (Zuweisungen)]** werden die Desktops und Pools angezeigt, denen die Anwendung gegenwärtig zugewiesen ist (einschließlich Installationstyp). Die Registerkarte **[Desktops]** zeigt die Desktops, die gegenwärtig mit der Anwendung verknüpft sind (einschließlich Installationsstatus). **Hinweis** Wenn Sie einem Pool eine ThinApp-Anwendung zuweisen, werden die Desktops im Pool auf der Registerkarte **[Desktops]** erst angezeigt, nachdem die Anwendung installiert ist.
Anzeigen aller ThinApp-Anwendungen, die einem bestimmten Desktop zugewiesen sind	Wählen Sie **[Inventory (Bestandsliste)]** > **[Desktops]** . Doppelklicken Sie anschließend in der Spalte **[Desktop]** auf den Namen des Desktops. Im ThinApps-Bereich auf der Registerkarte **[Summary (Übersicht)]** werden die einzelnen Anwendungen (einschließlich Installationsstatus) angezeigt, die dem Desktop gegenwärtig zugewiesen sind.
Anzeigen aller ThinApp-Anwendungen, die einem bestimmten Pool zugewiesen sind	Wählen Sie **[Inventory (Bestandsliste)]** > **[Pools]** . Doppelklicken Sie anschließend auf eine Pool-ID, wählen Sie die Registerkarte **[Inventory (Bestandsliste)]** und klicken Sie auf **[ThinApps]** . Im Fensterbereich mit den ThinApp-Zuweisungen werden die einzelnen Anwendungen angezeigt, die dem Pool gegenwärtig zugewiesen sind.

Installationsstatuswerte für ThinApp-Anwendungen

Nachdem Sie einem Desktop oder Pool eine ThinApp-Anwendung zugewiesen haben, zeigt View Administrator den Status der Installation an.

Tabelle 13-1 beschreibt die einzelnen Statuswerte.

Tabelle 13-1. Installationsstatus für ThinApp-Anwendungen

Status	Beschreibung
Assigned (Zugewiesen)	Die ThinApp-Anwendung wurde dem Desktop zugewiesen.
Install Error (Fehler bei der Installation)	Als View Administrator versucht hat, die ThinApp-Anwendung zu installieren, ist ein Fehler aufgetreten.
Uninstall Error (Fehler bei der Deinstallation)	Als View Administrator versucht hat, die ThinApp-Anwendung zu deinstallieren, ist ein Fehler aufgetreten.
Installed (Installiert)	Die ThinApp-Anwendung wurde installiert.
Pending Install (Ausstehende Installation)	View Administrator versucht, die ThinApp-Anwendung zu installieren. Die Zuweisung einer Anwendung mit diesem Status kann nicht aufgehoben werden. **Hinweis** Für Desktops in Pools wird dieser Wert nicht angezeigt.
Pending Uninstall (Ausstehende Deinstallation)	View Administrator versucht, die ThinApp-Anwendung zu deinstallieren.

Anzeigen von MSI-Paketinformationen

Nach dem Hinzufügen einer ThinApp-Anwendung zu View Administrator können Sie Informationen zu den MSI-Paketen anzeigen.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)]** > **[ThinApps]** .

Auf der Registerkarte **[Summary (Übersicht)]** werden die gegenwärtig verfügbaren Anwendungen sowie die Anzahl an vollständigen Zuweisungen und Streaming-Zuweisungen angezeigt.

2 Doppelklicken Sie in der Spalte **[ThinApp]** auf den Namen der Anwendung.

3 Wählen Sie die Registerkarte **[Summary (Übersicht)]** , um allgemeine Informationen zum MSI-Paket anzuzeigen.

4 Um detaillierte Informationen zum MSI-Paket anzuzeigen, klicken Sie auf **[Package Info (Paketinfo)]** .

Warten von ThinApp-Anwendungen in View Administrator

Das Verwalten von ThinApp-Anwendungen in View Administrator umfasst Aufgaben wie das Entfernen von ThinApp-Anwendungszuweisungen, ThinApp-Anwendungen und Anwendungs-Repositorys sowie das Ändern und Löschen von ThinApp-Vorlagen.

Hinweis Zum Aktualisieren einer ThinApp-Anwendung müssen Sie die ältere Version der Anwendung entfernen und eine neuere Version hinzufügen und zuweisen.

- Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktops auf Seite 280

  Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Desktops entfernt werden.

- Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop auf Seite 280

  Sie können Zuweisungen zu einer oder mehreren ThinApp-Anwendungen aus einem bestimmten Desktop entfernen.

- Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Pools auf Seite 281

  Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Pools entfernt werden.

- Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Pool auf Seite 281

  Sie können eine oder mehrere ThinApp-Anwendungszuweisungen aus einem bestimmten Pool entfernen.

- Entfernen einer ThinApp-Anwendung aus View Administrator auf Seite 281

  Wenn Sie eine ThinApp-Anwendung aus View Administrator entfernen, können Sie die Anwendung nicht länger Desktops und Pools zuweisen.

- Ändern oder Löschen einer ThinApp-Vorlage auf Seite 282

  Sie können Anwendungen zu einer ThinApp-Vorlage hinzufügen oder aus dieser entfernen. Eine ThinApp-Vorlage kann zudem gelöscht werden.

- Entfernen eines Anwendungs-Repository auf Seite 282

  Sie können ein Anwendungs-Repository aus View Administrator entfernen.

Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Desktops

Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Desktops entfernt werden.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Desktops darüber, dass die Anwendung entfernt werden soll.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)] > [ThinApps]** und doppelklicken Sie auf den Namen der ThinApp-Anwendung.

2 Wählen Sie auf der Registerkarte **[Assignments (Zuweisungen)]** einen Desktop und klicken Sie auf **[Remove Assignment (Zuweisung entfernen)]** .

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Desktops auszuwählen.

View Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

WICHTIG Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während View Administrator versucht, die Anwendung zu deinstallieren, schlägt die Deinstallation fehl und der Anwendungsstatus ändert sich in **[Uninstall Error (Fehler bei der Deinstallation)]** . Wenn dieser Fehler auftritt, müssen Sie die ThinApp-Anwendungsdateien zunächst manuell vom View-Desktop deinstallieren und anschließend in View Administrator auf **[Force Clear Assignment (Löschen der Zuweisung erzwingen)]** .

Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Desktop

Sie können Zuweisungen zu einer oder mehreren ThinApp-Anwendungen aus einem bestimmten Desktop entfernen.

Voraussetzungen

Benachrichtigen Sie die Benutzer des Desktops darüber, dass die Anwendungen entfernt werden sollen.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)] > [Desktops]** . Doppelklicken Sie anschließend in der Spalte **[Desktop]** auf den Namen des Desktops.

2 Wählen Sie auf der Registerkarte **[Summary (Übersicht)]** die ThinApp-Anwendung und klicken Sie im ThinApps-Fensterbereich auf **[Remove Assignment (Zuweisung entfernen)]** .

Wiederholen Sie diesen Schritt, um eine weitere Anwendungszuweisung zu entfernen.

View Administrator beginnt wenige Minuten später mit der Deinstallation der ThinApp-Anwendung.

WICHTIG Wenn ein Endbenutzer die ThinApp-Anwendung verwendet, während View Administrator versucht, die Anwendung zu deinstallieren, schlägt die Deinstallation fehl und der Anwendungsstatus ändert sich in **[Uninstall Error (Fehler bei der Deinstallation)]** . Wenn dieser Fehler auftritt, müssen Sie die ThinApp-Anwendungsdateien zunächst manuell vom View-Desktop deinstallieren und anschließend in View Administrator auf **[Force Clear Assignment (Löschen der Zuweisung erzwingen)]** klicken.

Entfernen einer ThinApp-Anwendungszuweisung aus mehreren Pools

Die Zuweisung zu einer bestimmten ThinApp-Anwendung kann aus einem oder mehreren Pools entfernt werden.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Desktops innerhalb der Pools darüber, dass die Anwendung entfernt werden soll.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)] > [ThinApps]** und doppelklicken Sie auf den Namen der ThinApp-Anwendung.

2 Wählen Sie auf der Registerkarte **[Assignments (Zuweisungen)]** einen Pool und klicken Sie auf **[Remove Assignment (Zuweisung entfernen)]** .

Sie können Strg+Klick oder Umschalt+Klick verwenden, um mehrere Pools auszuwählen.

View Administrator beginnt mit der Deinstallation der ThinApp-Anwendung, sobald sich ein Benutzer erstmalig an einem Desktop innerhalb des Pools anmeldet.

Entfernen mehrerer ThinApp-Anwendungszuweisungen aus einem Pool

Sie können eine oder mehrere ThinApp-Anwendungszuweisungen aus einem bestimmten Pool entfernen.

Voraussetzungen

Benachrichtigen Sie die Benutzer der Desktops innerhalb des Pools darüber, dass die Anwendungen entfernt werden sollen.

Vorgehensweise

1 Wählen Sie **[Inventory (Bestandsliste)] > [Pools]** und doppelklicken Sie auf die Pool-ID.

2 Klicken Sie auf der Registerkarte **[Inventory (Bestandsliste)]** auf **[ThinApps]** , wählen Sie die ThinApp-Anwendung und klicken Sie auf **[Remove Assignment (Zuweisung entfernen)]** .

Wiederholen Sie diesen Schritt, um mehrere Anwendungen zu entfernen.

View Administrator beginnt mit der Deinstallation der ThinApp-Anwendungen, sobald sich ein Benutzer erstmalig an einem Desktop innerhalb des Pools anmeldet.

Entfernen einer ThinApp-Anwendung aus View Administrator

Wenn Sie eine ThinApp-Anwendung aus View Administrator entfernen, können Sie die Anwendung nicht länger Desktops und Pools zuweisen.

Es kann erforderlich sein, eine ThinApp-Anwendung zu entfernen, wenn Ihre Organisation diese durch eine Anwendung eines anderen Anbieters ersetzen möchte.

Hinweis Das Entfernen einer ThinApp-Anwendung ist nicht möglich, wenn die Anwendung bereits einem Desktop oder Pool zugewiesen ist oder den Status **[Pending Uninstall (Ausstehende Deinstallation)]** aufweist.

Voraussetzungen

Wenn eine ThinApp-Anwendung gegenwärtig einem Desktop oder Pool zugewiesen ist, entfernen Sie die Zuweisung aus dem Desktop oder Pool.

Vorgehensweise

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** und wählen Sie die ThinApp-Anwendung aus.

2 Klicken Sie auf **[Remove ThinApp (ThinApp entfernen)]** .

3 Klicken Sie auf **[OK]** .

Ändern oder Löschen einer ThinApp-Vorlage

Sie können Anwendungen zu einer ThinApp-Vorlage hinzufügen oder aus dieser entfernen. Eine ThinApp-Vorlage kann zudem gelöscht werden.

Wenn Sie eine Anwendung zu einer ThinApp-Vorlage hinzufügen, nachdem die Vorlage einem Desktop oder Pool zugewiesen wurde, weist View Administrator die neue Anwendung nicht automatisch dem Desktop oder Pool zu. Beim Entfernen einer Anwendung aus einer ThinApp-Vorlage, die zuvor einem Desktop oder Pool zugewiesen wurde, wird die Zuweisung der Anwendung zum Desktop oder Pool beibehalten.

Vorgehensweise

◆ Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** und wählen Sie die ThinApp-Vorlage aus.

Option	Aktion
Hinzufügen oder Entfernen von ThinApp-Anwendungen aus einer Vorlage	Klicken Sie auf **[Edit Template (Vorlage bearbeiten)]** .
Löschen der Vorlage	Klicken Sie auf **[Delete Template (Vorlage löschen)]** .

Entfernen eines Anwendungs-Repository

Sie können ein Anwendungs-Repository aus View Administrator entfernen.

Möglicherweise ist es erforderlich, dass Sie ein Anwendungs-Repository entfernen, wenn Sie die darin enthaltenen MSI-Pakete nicht mehr benötigen oder Sie die MSI-Pakete auf eine andere Netzwerkfreigabe verschieben müssen. Der Freigabepfad eines Anwendungs-Repositorys in View Administrator kann nicht geändert werden.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [ThinApp Configuration (ThinApp-Konfiguration)]** und wählen Sie das Anwendungs-Repository aus.

2 Klicken Sie auf **[Remove Repository (Repository entfernen)]** .

Überwachen von und Fehlerbehebung bei ThinApp-Anwendungen in View Administrator

View Administrator protokolliert mit der ThinApp-Anwendungsverwaltung verbundene Ereignisse in der Datenbank für Ereignisse und Berichterstellung. Diese Ereignisse werden in View Administrator auf der Registerkarte **[Events (Ereignisse)]** angezeigt.

Auf der Registerkarte **[Events (Ereignisse)]** wird in folgenden Fällen ein Ereignis angezeigt:

- Eine ThinApp-Anwendung wird zugewiesen oder eine Anwendungszuweisung wird entfernt
- Eine ThinApp-Anwendung wird auf einem Desktop installiert oder deinstalliert
- Eine ThinApp-Anwendung kann nicht installiert oder deinstalliert werden

- Ein ThinApp-Anwendungs-Repository wird registriert, geändert oder aus View Administrator entfernt
- Eine ThinApp-Anwendung wird zu View Administrator hinzugefügt

Für häufige Probleme bei der ThinApp-Anwendungsverwaltung sind Tipps zur Fehlerbehebung verfügbar.

Keine Registrierung eines Anwendungs-Repositorys möglich

Sie können ein Anwendungs-Repository nicht in View Administrator registrieren.

Problem

Beim Versuch, ein Anwendungs-Repository in View Administrator zu registrieren, wird eine Fehlermeldung ausgegeben.

Ursache

Der View Connection Server-Host kann nicht auf die Netzwerkfreigabe zugreifen, auf der sich das Anwendungs-Repository befindet. Der im Textfeld **[Share path (Freigabepfad)]** eingegebene Pfad zur Netzwerkfreigabe ist möglicherweise falsch, die Netzwerkfreigabe mit dem Anwendungs-Repository befindet sich in einer Domäne, auf die nicht vom View Connection Server-Host aus zugegriffen werden kann, oder die Berechtigungen für die Netzwerkfreigabe wurden nicht ordnungsgemäß eingerichtet.

Lösung

- Wenn der Pfad zur Netzwerkfreigabe falsch ist, geben Sie den richtigen Pfad zur Netzwerkfreigabe ein. Pfade zu Netzwerkfreigaben, die IP-Adressen enthalten, werden nicht unterstützt.
- Gehört die Netzwerkfreigabe nicht zu einer Domäne, auf die zugegriffen werden kann, kopieren Sie Ihre Anwendungspakete auf eine Netzwerkfreigabe in einer Domäne, auf die der View Connection Server-Host zugreifen kann.
- Überprüfen Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe **[Domain Computers (Domänencomputer)]** Lesezugriff zu gewähren. Wenn Sie ThinApps zu Domänencontrollern zuweisen möchten, stellen Sie sicher, dass die Datei- und Freigabeberechtigungen auch der integrierten Active Directory-Gruppe **[Domain Computers (Domänencomputer)]** Lesezugriff gewähren. Nachdem Sie Berechtigungen festgelegt oder geändert haben, kann es bis zu 20 Minuten dauern, bis die Netzwerkfreigabe verfügbar ist.

Kein Hinzufügen von ThinApp-Anwendungen zu View Administrator möglich

View Administrator kann keine ThinApp-Anwendungen zu View Administrator zuweisen.

Problem

Beim Klicken auf **[Scan New ThinApps (Neue ThinApps durchsuchen)]** in View Administrator sind keine MSI-Pakete verfügbar.

Ursache

Die Anwendungspakete liegen entweder nicht im MSI-Format vor oder der View Connection Server-Host kann nicht auf die Verzeichnisse auf der Netzwerkfreigabe zugreifen.

Lösung

- Stellen Sie sicher, dass die Anwendungspakete im Anwendungs-Repository im MSI-Format vorliegen.
- Stellen Sie sicher, dass die Netzwerkfreigabe die View-Anforderungen für ThinApp-Anwendungen erfüllt. Weitere Informationen finden Sie unter „View-Anforderungen für ThinApp-Anwendungen“, auf Seite 267.

- Stellen Sie sicher, dass für die Verzeichnisse auf der Netzwerkfreigabe die richtigen Berechtigungen festgelegt wurden. Weitere Informationen finden Sie unter „Keine Registrierung eines Anwendungs-Repositorys möglich“, auf Seite 283.

Während ein Anwendungs-Repository durchsucht wird, werden Meldungen in der Debug-Protokolldatei von View Connection Server aufgeführt. View Connection Server-Protokolldateien befinden sich auf dem View Connection Server-Host im Verzeichnis *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Kein Zuweisen einer ThinApp-Vorlage möglich

Eine ThinApp-Vorlage kann keinem Desktop oder Pool zugewiesen werden.

Problem

View Administrator gibt beim Versuch, eine ThinApp-Vorlage einem Desktop oder Pool zuzuweisen, einen Zuweisungsfehler zurück.

Ursache

Die ThinApp-Vorlage enthält entweder eine Anwendung, die dem Desktop oder Pool bereits zugewiesen wurde, oder die ThinApp-Vorlage wurde dem Desktop oder Pool bereits mit einem anderen Installationstyp zugewiesen.

Lösung

Wenn die Vorlage eine ThinApp-Anwendung enthält, die dem Desktop oder Pool bereits zugewiesen wurde, erstellen Sie eine neue Vorlage ohne diese Anwendung oder entfernen Sie die Anwendung aus der vorhandenen Vorlage. Weisen Sie die neue oder geänderte Vorlage dem Desktop oder Pool zu.

Um den Installationstyp einer ThinApp-Anwendung zu ändern, muss die vorhandene Anwendungszuweisung aus dem Desktop oder Pool entfernt werden. Nach der Deinstallation der ThinApp-Anwendung können Sie diese dem Desktop oder Pool mit einem anderen Installationstyp zuweisen.

ThinApp-Anwendung wird nicht installiert

View Administrator kann eine ThinApp-Anwendung nicht installieren.

Problem

Der Installationsstatus einer ThinApp-Anwendung weist entweder auf eine ausstehende Installation oder auf einen Fehler bei der Installation hin.

Ursache

Folgendes sind häufige Ursachen für dieses Problem:

- Es war nicht genügend Speicherplatz vorhanden, um die ThinApp-Anwendung auf dem Desktop zu installieren.
- Die Netzwerkverbindung zwischen View Connection Server-Host und Desktop bzw. zwischen View Connection Server-Host und Anwendungs-Repository wurde getrennt.
- Ein Zugriff auf die ThinApp-Anwendung auf der Netzwerkfreigabe war nicht möglich.
- Die ThinApp-Anwendung wurde bereits installiert oder das Verzeichnis bzw. die Datei ist bereits auf dem Desktop vorhanden.

In den View Agent- und View Connection Server-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

View Agent-Protokolldateien befinden sich auf dem Desktop im Verzeichnis *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs (auf Windows XP-Systemen) und im Verzeichnis *Laufwerk*:\Programme\VMware\VDM\logs (auf Windows 7-Systemen).

View Connection Server-Protokolldateien befinden sich auf dem View Connection Server-Host im Verzeichnis *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** .

2 Klicken Sie auf den Namen der ThinApp-Anwendung.

3 Wählen Sie auf der Registerkarte **[Desktops]** den Desktop aus und klicken Sie auf **[Retry Install (Erneuter Installationsversuch)]** , um die ThinApp-Anwendung erneut zu installieren.

ThinApp-Anwendung wird nicht deinstalliert

View Administrator kann eine ThinApp-Anwendung nicht deinstallieren.

Problem

Der Installationsstatus einer ThinApp-Anwendung weist auf einen Fehler bei der Deinstallation hin.

Ursache

Folgendes sind häufige Ursachen für diesen Fehler:

- Die ThinApp-Anwendung wurde verwendet, als View Administrator versucht hat, sie zu deinstallieren.
- Die Netzwerkverbindung zwischen View Connection Server-Host und Desktop wurde getrennt.

In den View Agent- und View Connection Server-Protokolldateien finden Sie weitere Informationen zur Ursache des Problems.

View Agent-Protokolldateien befinden sich auf dem Desktop im Verzeichnis *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs (auf Windows XP-Systemen) und im Verzeichnis *Laufwerk*:\Programme\VMware\VDM\logs (auf Windows 7-Systemen).

View Connection Server-Protokolldateien befinden sich auf dem View Connection Server-Host im Verzeichnis *Laufwerk*:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\logs.

Lösung

1 Wählen Sie in View Administrator **[Inventory (Bestandsliste)] > [ThinApps]** .

2 Klicken Sie auf den Namen der ThinApp-Anwendung.

3 Klicken Sie auf die Registerkarte **[Desktops]** , wählen Sie den Desktop aus und klicken Sie auf **[Retry Uninstall (Erneuter Deinstallationsversuch)]** , um den Deinstallationsvorgang erneut auszuführen.

4 Schlägt die Deinstallation erneut fehl, entfernen Sie die ThinApp-Anwendung manuell aus dem Desktop und klicken Sie anschließend auf **[Force Clear Assignment (Löschen der Zuweisung erzwingen)]** .

   Über diesen Befehl wird die ThinApp-Anwendungszuweisung in View Administrator gelöscht. Dateien oder Einstellungen im Desktop werden nicht entfernt.

   WICHTIG Verwenden Sie diesen Befehl nur nach dem manuellen Entfernen der ThinApp-Anwendung aus dem Desktop.

MSI-Paket ist ungültig

View Administrator meldet ein ungültiges MSI-Paket in einem Anwendungs-Repository.

Problem

View Administrator meldet während eines Vorgangs zum Durchsuchen ein ungültiges MSI-Paket.

Ursache

Folgendes sind häufige Ursachen für dieses Problem:

- Die MSI-Datei ist beschädigt.
- Die MSI-Datei wurde nicht mit ThinApp erstellt.
- Die MSI-Datei wurde mit einer nicht unterstützten Version von ThinApp erstellt oder erneut paketiert. Sie müssen ThinApp Version 4.6 oder höher verwenden.

Lösung

Weitere Informationen zum Beheben von Problemen mit MSI-Paketen finden Sie im *ThinApp-Benutzerhandbuch*.

ThinApp-Konfigurationsbeispiel

In diesem ThinApp-Konfigurationsbeispiel werden alle Schritte einer typischen ThinApp-Konfiguration beschrieben, angefangen beim Erstellen von Anwendungspaketen bis hin zum Überprüfen des Status einer Installation.

Voraussetzungen

Vollständige Informationen zum Ausführen der Schritte in diesem Beispiel finden Sie in den folgenden Themen.

- „Erfassen und Speichern von Anwendungspaketen“, auf Seite 268
- „Zuweisen von ThinApp-Anwendungen zu Desktops und Pools“, auf Seite 272

Vorgehensweise

1. Laden Sie die ThinApp-Software von der Seite http://www.vmware.com/de/products/thinapp herunter und installieren Sie sie auf einem Computer, auf dem noch keine Version dieser Software vorhanden ist.

   View unterstützt ThinApp 4.6 und höher.

2. Verwenden Sie den ThinApp Setup Capture-Assistenten zum Erstellen von Anwendungspaketen im MSI-Format.

3. Erstellen Sie eine Ordnerfreigabe auf einem Computer in einer Active Directory-Domäne, auf die der View Connection Server-Host und Ihre View-Desktops zugreifen können, und konfigurieren Sie die Datei- und Freigabeberechtigungen für die Ordnerfreigabe, um der integrierten Active Directory-Gruppe **[Domain Computers (Domänencomputer)]** Lesezugriff zu gewähren.

   Wenn Sie Domänencontrollern ThinApp-Anwendungen zuweisen möchten, müssen Sie der integrierten Active Directory-Gruppe **[Domain Controllers (Domänencontroller)]** Lesezugriff gewähren.

4. Kopieren Sie die MSI-Pakete in den freigegebenen Ordner.

5. Registrieren Sie den freigegebenen Ordner als Anwendungs-Repository in View Administrator.

6. Durchsuchen Sie die MSI-Pakete im Anwendungs-Repository in View Administrator und fügen Sie ausgewählte ThinApp-Anwendungen zu View Administrator hinzu.

7 Legen Sie fest, ob die ThinApp-Anwendungen Desktops oder Pools zugewiesen werden sollen.

Wenn Sie eine allgemeine Benennungskonvention für Ihre Desktops verwenden, können Sie Anwendungen mithilfe von Desktop-Zuweisungen schnell auf alle Desktops mit derselben Benennungskonvention verteilen. Wenn Sie Pools nach Abteilung oder Benutzertyp organisieren, können Sie Anwendungen mithilfe von Pool-Zuweisungen schnell an bestimmte Abteilungen oder Benutzer verteilen.

8 Wählen Sie die ThinApp-Anwendungen in View Administrator aus, die Ihren Desktops oder Pools zugewiesen werden sollen, und geben Sie die Installationsmethode an.

Option	Aktion
Streaming	Installiert eine Verknüpfung zur Anwendung auf dem Desktop. Die Verknüpfung verweist auf die Anwendung auf der Netzwerkfreigabe, auf der sich das Repository befindet. Zur Ausführung der Anwendung müssen Benutzer über Zugriff auf die Netzwerkfreigabe verfügen.
Full (Vollständig)	Installiert die vollständige Anwendung auf dem lokalen Dateisystem.

9 Überprüfen Sie in View Administrator den Installationsstatus der ThinApp-Anwendungen.

14 Verwalten von lokalen Desktops

Zur Verwaltung von Desktops, die im lokalen Modus verwendet werden, müssen Sie die Umgebung so einrichten, dass Daten übertragen werden, wenn Benutzer ihre View-Desktops auf lokale Systeme auschecken. Sie müssen auch andere Aufgaben ausführen, die Datenübertragungen erfordern, wie z.B. das Einchecken eines Desktops, das Rollback sowie die Sicherung. Darüber hinaus müssen Sie Richtlinien festlegen, in denen angegeben wird, welche dieser Aufgaben von den Benutzern initiiert werden können.

Dieses Kapitel behandelt die folgenden Themen:

- „Vorteile bei der Verwendung von View-Desktops im lokalen Modus“, auf Seite 289
- „Verwalten von View Transfer Server“, auf Seite 297
- „Verwalten des Transfer Server-Repositorys“, auf Seite 302
- „Verwalten von Datenübertragungen“, auf Seite 309
- „Konfigurieren von Sicherheits- und Optimierungseinstellungen für lokale Desktop-Vorgänge“, auf Seite 313
- „Konfigurieren der Ressourcennutzung für Endpunkte“, auf Seite 318
- „Konfigurieren eines HTTP-Caches für die Bereitstellung lokaler Desktops über ein WAN“, auf Seite 323
- „Konfigurieren des Taktsignalintervalls für Clientcomputer mit lokalem Desktop“, auf Seite 327
- „Manuelles Herunterladen eines lokalen Desktops an einem Standort mit unzureichenden Netzwerkverbindungen“, auf Seite 328
- „Fehlerbehebung bei View Transfer Server- und lokalen Desktop-Vorgängen“, auf Seite 332

Vorteile bei der Verwendung von View-Desktops im lokalen Modus

Bei Verwendung von View Client with Local Mode können Benutzer einen View-Desktop auschecken und auf ein lokales System (z. B. ein Laptop) herunterladen. Administratoren können diese lokalen View-Desktops durch das Festlegen von Richtlinien verwalten. So kann der Administrator beispielsweise die Häufigkeit von Sicherungen und Serververbindungen sowie den Zugriff auf USB-Geräte festlegen und Berechtigungen zum Einchecken von Desktops gewähren.

Für Mitarbeiter in externen Büros mit schlechter Netzwerkverbindung werden Anwendungen schneller auf einem lokalen View-Desktop als auf einem Remote-Desktop ausgeführt. Außerdem können Benutzer die lokale Desktop-Version mit oder ohne Netzwerkverbindung nutzen.

Wenn auf dem Clientsystem eine Netzwerkverbindung besteht, kommuniziert der ausgecheckte Desktop weiterhin mit View Connection Server, um Richtlinienaktualisierungen bereitzustellen und sicherzustellen, dass die lokal zwischengespeicherten Authentifizierungskriterien auf dem neuesten Stand sind. Standardmäßig wird alle fünf Minuten ein Kontaktversuch unternommen.

View-Desktops im lokalen Modus verhalten sich genauso wie die entsprechenden Remote-Desktops, können jedoch lokale Ressourcen nutzen. Wartezeiten werden vermieden und die Leistung wird verbessert. Benutzer können die Verbindung zu ihrem lokalen View-Desktop trennen und sich erneut anmelden, ohne sich mit View Connection Server zu verbinden. Sobald der Netzwerkzugriff wiederhergestellt oder der Benutzer bereit ist, kann die ausgecheckte virtuelle Maschine gesichert, per Rollback zurückgesetzt oder eingecheckt werden.

Nutzung lokaler Ressourcen

Nach dem Auschecken eines lokalen Desktops kann dieser den Arbeitsspeicher und die CPU des lokalen Systems nutzen. Zusätzliche verfügbare Arbeitsspeicherkapazität, die über die erforderliche Arbeitsspeichergröße für das Host- und Gastbetriebssystem hinausgeht, wird z. B. üblicherweise unabhängig von den in vCenter Server für die virtuelle Maschine festgelegten Arbeitsspeichereinstellungen zwischen Host und lokalem View-Desktop aufgeteilt. In gleicher Weise kann der lokale View-Desktop automatisch bis zu zwei auf dem lokalen System verfügbare CPUs nutzen, und Sie können den lokalen Desktop für die Verwendung von bis zu vier CPUs konfigurieren.

Auch wenn ein lokaler Desktop lokale Ressourcen nutzen kann, kann ein Desktop unter Windows 7 oder Windows Vista View, der auf einem ESX/ESXi 3.5-Host erstellt wurde, keine 3D- und Windows Aero-Effekte produzieren. Diese Einschränkung gilt auch dann, wenn der Desktop zur lokalen Verwendung auf einem Windows 7- oder Windows Vista-Host ausgecheckt wird. Windows Aero- und 3D-Effekte stehen nur dann zur Verfügung, wenn der View-Desktop mithilfe von vSphere 4.x oder höher erstellt wird.

Einsparen von Rechenzentrumsressourcen, indem die Verwendung des lokalen Modus als obligatorisch festgelegt wird

Sie können die Rechenzentrumskosten für Bandbreiten-, Arbeitsspeicher- und CPU-Ressourcen reduzieren, indem Sie festlegen, dass View-Desktops heruntergeladen und ausschließlich im lokalen Modus verwendet werden können. Diese Strategie wird gelegentlich als „Bring your own PC“-Initiative für interne und externe Mitarbeiter bezeichnet.

Auschecken

Wenn der View-Desktop ausgecheckt wird, wird in vCenter ein Snapshot erstellt, um den Status der virtuellen Maschine zu speichern. Die vCenter Server-Version des Desktops wird gesperrt, sodass keine anderen Benutzer darauf zugreifen können. Bei einem gesperrten View-Desktop werden vCenter Server-Operationen deaktiviert. Hierzu gehören Operationen wie das Einschalten des Online-Desktops, das Erstellen von Snapshots und die Bearbeitung der Einstellungen der virtuellen Maschine. View-Administratoren können jedoch die lokale Sitzung dennoch überwachen und auf die vCenter Server-Version zugreifen, um den Zugriff zu entfernen oder ein Rollback für den Desktop durchzuführen.

Sicherungen

Während Sicherungen wird auf dem Clientsystem ein Snapshot erstellt, um den Status der ausgecheckten virtuellen Maschine beizubehalten. Die Deltadaten zwischen diesem Snapshot und dem Snapshot in vCenter werden nach vCenter repliziert und dort mit dem Snapshot zusammengeführt. Der View-Desktop in vCenter Server wird mit allen neuen Daten und Konfigurationen aktualisiert, der lokale Desktop bleibt auf dem lokalen System jedoch ausgecheckt und die Sperre wird in vCenter Server beibehalten.

Rollbacks Bei einem Rollback wird der lokale View-Desktop verworfen und die Sperre wird in vCenter Server aufgehoben. Nachfolgende Clientverbindungen werden an den View-Desktop in vCenter Server weitergeleitet, bis der Desktop wieder ausgecheckt wird.

Einchecken Wenn ein View-Desktop eingecheckt wird, wird auf dem Clientsystem ein Snapshot erstellt, um den Status der virtuellen Maschine zu speichern. Die Deltadaten zwischen diesem Snapshot und dem Snapshot in vCenter werden nach vCenter repliziert und dort mit dem Snapshot zusammengeführt. Die Sperre der virtuellen Maschine in vCenter Server wird aufgehoben. Nachfolgende Clientverbindungen werden an den View-Desktop in vCenter Server weitergeleitet, bis der Desktop wieder ausgecheckt wird.

Die Daten auf den einzelnen lokalen Systemen werden mit AES verschlüsselt. Die 128-Bit-Verschlüsselung wird standardmäßig verwendet, Sie können jedoch auch die 192-Bit- oder die 256-Bit-Verschlüsselung konfigurieren. Der Desktop besitzt eine über Richtlinien gesteuerte Lebenszeit. Wenn der Client den Kontakt mit View Connection Server verliert, entspricht die maximale Zeit ohne Serverkontakt dem Zeitraum, während dessen der Benutzer den Desktop weiterhin nutzen kann, bevor ihm der Zugriff verweigert wird. In ähnlicher Weise ist das Clientsystem nach Entfernen des Benutzerzugriffs nicht mehr zugänglich, wenn der Cache abläuft oder nachdem der Client diese Änderung durch View Connection Server ermittelt hat.

Für View Client with Local Mode gelten folgende Einschränkungen:

- Sie müssen eine View-Lizenz besitzen, die die Local Mode-Komponente umfasst.
- Benutzer können während Rollbacks und Vorgängen zum Auschecken nicht auf ihren lokalen Desktop zugreifen.
- Diese Funktion steht nur für virtuelle Maschinen zur Verfügung, die von vCenter Server verwaltet werden.
- Das Auschecken eines View-Desktops, der virtuelle Hardware der Version 8 verwendet, wird nicht unterstützt. Wenn Sie vSphere 5 zum Erstellen virtueller Maschinen verwenden, die als Quellen für Desktops im lokalen Modus verwendet werden sollen, erstellen Sie unbedingt virtuelle Maschinen, die virtuelle Hardware der Version 7 verwenden.
- Für Desktops, die im lokalen Modus ausgeführt werden, kann View Persona-Verwaltung nicht verwendet werden.
- Die Zuweisung von Anwendungspaketen, die mit VMware ThinApp erstellt wurden, wird für heruntergeladene und im lokalen Modus verwendete View-Desktops nicht unterstützt. Ein Rollback eines Desktops kann dazu führen, dass View Connection Server nicht die richtigen Informationen zu den ThinApps auf diesem Desktop vorliegen.
- Aus Sicherheitsgründen können Sie innerhalb des View-Desktops nicht auf die Host-CD-ROM zugreifen.
- Ebenfalls aus Sicherheitsgründen können Sie keinen Text oder Systemobjekte wie Dateien und Ordner zwischen dem lokalen System und dem View-Desktop kopieren und einfügen.

Übersicht über die Einrichtung einer Bereitstellung lokaler Desktops

Für die Erstellung und Bereitstellung von View-Desktops im lokalen Modus müssen Sie über die erforderliche Lizenz verfügen, eine View Transfer Server-Instanz einrichten, eine von vCenter Server verwaltete Desktop-Quelle verwenden sowie für den lokalen Modus spezifische Einstellungen und Richtlinien anwenden.

Wenn Sie Desktops erstellen, die zur Verwendung auf lokalen Systemen von Endbenutzern ausgecheckt werden können, müssen neben den üblichen Einrichtungsschritten mehrere Aufgaben für den lokalen Modus ausgeführt werden.

1 Stellen Sie sicher, dass Sie über eine Lizenz für VMware View Client with Local Mode verfügen.

   Wechseln Sie in View Administrator zu **[View Configuration (View-Konfiguration)] > [Product licensing and usage (Produktlizenzierung und -verwendung)]** .

2 Stellen Sie sicher, dass das für den Zugriff auf vCenter Server aus View Connection Server verwendete Benutzerkonto über die erforderlichen Administratorrechte verfügt.

   Um das verwendete Benutzerkonto anzuzeigen, navigieren Sie in View Administrator zu **[View Configuration (View-Konfiguration)] > [Server]** . Wählen Sie anschließend die vCenter Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .

   Die Liste der erforderlichen Berechtigungen zum Ausführen von vCenter Server-Vorgängen ist im Dokument *Installation von VMware View* im Abschnitt zur Konfiguration von Benutzerkonten für vCenter Server enthalten.

3 Installieren Sie View Transfer Server in einer virtuellen Maschine und fügen Sie diesen Server zu einer View Connection Server-Konfiguration hinzu.

   Wechseln Sie in View Administrator zu **[View Configuration (View-Konfiguration)] > [Server]** .

4 Wenn Sie Linked-Clone-Desktops aus View Composer verwenden möchten, konfigurieren Sie ein Transfer Server-Repository.

   Wechseln Sie in View Administrator zu **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

5 Wenn ein manueller Pool erstellt werden soll, müssen Sie sicherstellen, dass es sich bei der Desktop-Quelle um eine virtuelle Maschine handelt, die von vCenter Server verwaltet wird.

6 Erstellen Sie in vCenter Server eine virtuelle Maschine, die als Desktop-Quelle verwendet werden soll.

   Wenn Sie eine virtuelle Maschine erstellen, die über einen größeren virtuellen Arbeitsspeicher und mehr virtuelle Prozessoren verfügt, als auf einem lokalen Clientsystem verfügbar sind, wird die lokale Version des Desktops nicht gestartet und es wird eine Fehlermeldung angezeigt.

7 Wenn Sie Linked-Clone-Desktops verwenden möchten, veröffentlichen Sie das View Composer-Basis-Image des Desktops als Paket im Transfer Server-Repository.

   Sie können das Basis-Image veröffentlichen, wenn Sie einen Pool erstellen oder nachdem der Pool erstellt wurde.

8 Stellen Sie sicher, dass der Wert der Richtlinie **[Local Mode (Lokaler Modus)]** für den Desktop-Pool auf **[Allow (Zulassen)]** gesetzt ist.

   Navigieren Sie in View Administrator auf die Registerkarte **[Policies (Richtlinien)]** für diesen Pool.

9 Wenn Desktops ausschließlich im lokalen Modus ausgeführt werden sollen, sodass Benutzer die Desktops immer auschecken müssen, setzen Sie die Richtlinie **[Remote Mode (Remote-Modus)]** auf **[Deny (Ablehnen)]** .

   Navigieren Sie in View Administrator auf die Registerkarte **[Policies (Richtlinien)]** für diesen Pool.

10 Weisen Sie die Endbenutzer an, auf den lokalen Systemen View Client with Local Mode zu installieren.

WICHTIG Zusätzlich sollten Sie bei der Planung einer Bereitstellung lokaler Desktops Folgendes berücksichtigen:

- Wenn Sie automatisierte Pools erstellen, nehmen Sie eine dedizierte Zuweisung vor und erstellen Sie den Pool nur für Desktops, die im lokalen Modus verwendet werden sollen. Virtuelle Maschinen, die für eine Verwendung im lokalen Modus vorgesehen sind, können in Datenspeichern mit niedrigerer Anzahl an E/A-Vorgängen pro Sekunde (IOPS) platziert werden in Speichern, die eine große Anzahl an Remote-View-Desktops unterstützen sollen. Da das Zuweisen von ThinApp-Paketen zu lokalen Desktops nicht unterstützt wird, wird außerdem empfohlen, ThinApp-Pakete nur zu Pools zuzuweisen, die keine lokalen Desktops enthalten.
- Als standardmäßige Vorgehensweise für Desktops wird empfohlen, auf jedem View-Desktop, der im lokalen Modus verwendet werden soll, ein eindeutiges Passwort für das lokale Administratorkonto zu erstellen.
- Wird der Desktop für die Verwendung der RSA-Authentifizierung konfiguriert, müssen Endbenutzer das RSA-Token bereitstellen, wenn eine Netzwerkverbindung mit View Connection Server besteht. Ist keine Netzwerkverbindung vorhanden, müssen Sie dieses nicht bereitstellen.

Festlegen eines Desktops zur ausschließlichen Ausführung im lokalen Modus

Sie können die Rechenzentrumskosten für Bandbreiten-, Arbeitsspeicher- und CPU-Ressourcen reduzieren, indem Sie festlegen, dass View-Desktops heruntergeladen und ausschließlich im lokalen Modus ausgeführt werden können.

Wenn ein View-Desktop so konfiguriert ist, dass er ausschließlich im lokalen Modus ausgeführt werden kann, wird den Benutzern bei Auswahl des Desktops in View Client angezeigt, dass der Desktop heruntergeladen und ausgecheckt werden muss. Die Optionen für die Verbindungsherstellung mit dem Desktop und das Einchecken sind für die Endbenutzer nicht verfügbar.

Voraussetzungen

- Stellen Sie sicher, dass der View-Desktop sämtliche Anforderungen für die Ausführung im lokalen Modus erfüllt.

  Siehe „Übersicht über die Einrichtung einer Bereitstellung lokaler Desktops“, auf Seite 292.
- Machen Sie sich mit den Richtlinien und Einstellungen für den lokalen Modus vertraut.

  Siehe „Verwalten von Datenübertragungen“, auf Seite 309.

Vorgehensweise

1 Zeigen Sie in View Administrator die Richtlinie für die geeignete Ebene an.

Option	Aktion
Alle Desktops und Pools	Wählen Sie **[Policies (Richtlinien)] > [Global Policies (Globale Richtlinien)] > [View-Richtlinien]** und klicken Sie auf **[Edit Policies (Richtlinien bearbeiten)]** .
Einzelne Pools	Wählen Sie **[Inventory (Bestandsliste)] > [Pools] > [*spezifischer_Pool*]** . Klicken Sie auf der Registerkarte **[Policies (Richtlinien)]** im Bereich **[View Policies (Richtlinien anzeigen)]** auf **[Edit Policies (Richtlinien bearbeiten)]** .
Einzelner Benutzer	Wählen Sie **[Inventory (Bestandsliste)] > [Pools] > [*spezifischer_Pool*]** . Klicken Sie dann auf der Registerkarte **[Policies (Richtlinien)]** auf **[User Overrides (Außerkraftsetzungen durch Benutzer)]** .

2 Setzen Sie die View-Richtlinie **[Remote Mode (Remote-Modus)]** auf **[Deny (Ablehnen)]** .

Option	Aktion
Alle Desktops und Pools oder ein einzelner Pool	Legen Sie im Dialogfeld zum Bearbeiten von View-Richtlinien für **[Remote Mode (Remote-Modus)]** die Option **[Deny (Ablehnen)]** fest und klicken Sie anschließend auf **[OK]** .
Einzelner Benutzer	Führen Sie die Schritte des Assistenten zum Hinzufügen von Benutzern aus, um den Benutzer anzugeben, und setzen Sie **[Remote Mode (Remote-Modus)]** auf **[Deny (Ablehnen)]** .

Der Desktop muss nun heruntergeladen und ausgecheckt werden.

Weiter

Wenn Sie Benutzer am erneuten Einchecken des Desktops hindern möchten, legen Sie die Richtlinie **[User-initiated check in (Vom Benutzer initiiertes Einchecken)]** auf **[Deny (Ablehnen)]** fest.

Wenn Sie Benutzer daran hindern möchten, ein Rollback für den Desktop durchzuführen, legen Sie die Richtlinie **[User-initiated rollback (Benutzer-initiiertes Rollback)]** auf **[Deny (Ablehnen)]** fest.

Erstmaliges Auschecken eines Desktops im lokalen Modus

Wenn ein Endbenutzer einen View-Desktop erstmalig zur Verwendung im lokalen Modus auscheckt, umfasst der Vorgang zum Auschecken und Herunterladen mehrere Phasen und diese Schritte dauern länger als bei nachfolgenden Auscheckvorgängen.

Wenn sich ein Endbenutzer bei View Client anmeldet und eine Liste mit Desktops anzeigt wird, kann der Benutzer sich entweder mit einem Desktop verbinden und diesen auschecken oder den Desktop auschecken, ohne zunächst eine Remote-Verbindung herzustellen.

WICHTIG Sie können einen Desktop nicht auschecken, wenn Sie bei der Anmeldung die Funktion **[Log in as current user (Anmelden als aktueller Benutzer)]** gewählt haben. Sie müssen View Client schließen, erneut starten und das Kontrollkästchen **[Log in as current user (Anmelden als aktueller Benutzer)]** deaktivieren.

Wenn der Endbenutzer eine Verbindung mit dem Desktop herstellt und diesen auscheckt, wird der Benutzer vom Remote-Desktop abgemeldet, die virtuelle Maschine im Rechenzentrum wird gesperrt und eine Kopie der virtuellen Maschine wird für den Endbenutzer heruntergeladen.

Nach dem Herunterladen werden beim erstmaligen Einschalten des lokalen Desktops durch den Endbenutzer verschiedene Treiber auf dem lokalen Desktop installiert. Welche Treiber installiert werden, hängt vom Betriebssystem des View-Desktops sowie von der Hardware und vom Betriebssystem des lokalen Computers ab. Während der Treiberinstallation ist die Leistung des View-Desktops beeinträchtigt. Dies gilt insbesondere, wenn auf dem View-Desktop ein Windows XP-Betriebssystem ausgeführt wird.

Im Anschluss an die Treiberinstallation wird der Endbenutzer zum Neustart des lokalen Desktops aufgefordert.

HINWEIS Wenn Sie beim Starten oder Herunterfahren des Gastbetriebssystems in ein View-Desktop-Fenster klicken, kann es vorkommen, dass die Zeigersteuerung im Fenster verbleibt. Nachdem alle Startvorgänge abgeschlossen sind und die VMware Tools ausgeführt werden, wird der Zeiger freigegeben. Wenn die Zeigersteuerung weiterhin im Desktop-Fenster verbleibt, können Sie den Zeiger durch Drücken von Strg+Alt freigeben.

Die RAM-Größe und die Anzahl an CPUs, die der lokale View-Desktop nutzt, richtet sich nach der Kapazität des lokalen Computers. Da der View-Desktop NAT verwendet, werden die IP- und MAC-Adressen des lokalen Computers gemeinsam verwendet. Weitere Informationen finden Sie unter „Konfigurieren der Ressourcennutzung für Endpunkte“, auf Seite 318.

Empfohlene Vorgehensweisen für das Bereitstellen lokaler Desktops

Die empfohlenen Vorgehensweisen betreffen Fragen zu Arbeitsspeicher, Rechenleistung und verschiedene Komponenten, die sich auf eine Bereitstellung im lokalen Modus auswirken.

Allgemeine Empfehlungen für die meisten Bereitstellungen

Konfiguration der virtuellen Maschine

Desktops, die im lokalen Modus ausgeführt werden, nehmen basierend auf den verfügbaren Ressourcen des Clientcomputers eine automatische Anpassung von Arbeitsspeichermenge und Rechenleistung vor. Aufgrund dieser Fähigkeit können Sie beim Erstellen der virtuellen Maschine in vCenter Server die Mindestmenge an RAM und virtuellen CPUs konfigurieren, die für das Gastbetriebssystem erforderlich sind.

View Transfer Server

Einige Funktionen von View Transfer Server sind CPU-intensiv. Wenn Sie für Vorgänge im lokalen Modus SSL einsetzen möchten, beispielsweise für das Ein- und Auschecken von Desktops oder für das Replizieren von Daten in das Rechenzentrum, benötigt die virtuelle Maschine, die Transfer Server hostet, möglicherweise eine zusätzliche virtuelle CPU. Wenn Sie die Komprimierung für Replikationsvorgänge aktivieren, benötigen Sie möglicherweise auch mehr Rechenleistung. Angaben zu den Mindestanforderungen für Arbeitsspeicher und Prozessor finden Sie im Kapitel zu den View Transfer Server-Systemanforderungen im Dokument *Installation von VMware View*.

Die Anzahl der zu View Connection Server hinzugefügten View Transfer Server-Instanzen richtet sich danach, wie wichtig eine hohe Verfügbarkeit ist. Wenn Sie eine hohe Verfügbarkeit wünschen, fügen Sie mindestens zwei Instanzen hinzu. Falls eine View Transfer Server-Instanz ausfällt, sendet View Connection Server Anforderungen automatisch an die zweite Instanz.

Zur Berechnung der benötigten Transfer Server-Instanzen müssen Sie außerdem berücksichtigen, wie viele Endbenutzer gleichzeitig Daten replizieren oder Desktops ein- und auschecken. Jede View Transfer Server-Instanz kann bis zu 60 gleichzeitige Festplattenvorgänge unterstützen, wobei die Netzwerkbandbreite wahrscheinlich bereits bei einer niedrigeren Anzahl erschöpft ist. VMware hat 20 gleichzeitige Festplattenvorgänge getestet, beispielsweise 20 Clients, die gleichzeitig einen lokalen Desktop über eine Netzwerkverbindung mit 1 GB pro Sekunde herunterladen.

Transfer Server-Repository

Basis-Images von View Composer-Linked-Clone-Desktops werden im Transfer Server-Repository auf einer Netzwerkfreigabe gespeichert. Je schneller Ihre Netzwerkfestplatten sind, desto besser ist die Leistung.

Pool-Einstellungen

Verwenden Sie View Composer, um Linked-Clone-Desktop-Pools zu erstellen. Wenn Sie den Assistenten zum Erstellen von Pools verwenden, nehmen Sie eine dedizierte Zuweisung vor und erstellen Sie den Pool nur für Desktops, die im lokalen Modus verwendet werden sollen. Virtuelle Maschinen im lokalen Modus können in Datenspeichern mit niedrigerer Anzahl an E/A-Vorgängen pro Sekunde gespeichert werden in Speichern, die eine große Anzahl von Remote-View-Desktops unterstützen sollen.

Datenreplikation

Ermitteln Sie, ob Endbenutzer Daten von Betriebssystemfestplatten replizieren müssen, beispielsweise die Daten einer Anpassungsspezifikation. Falls nicht, legen Sie eine Richtlinie fest, sodass nur persistente Festplatten repliziert werden.

Wenn Sie ein Intervall für die automatische Replikation festlegen, verwenden Sie das Standardintervall von 12 Stunden oder legen Sie ein noch größeres Intervall fest.

Aktivieren Sie die Deduplizierung oder Komprimierung nur dann, wenn aufgrund einer langsamen Netzwerkverbindung Probleme auftreten. Die Funktionen für Deduplizierung und Komprimierung verringern die benötigte Bandbreite, erfordern jedoch auch mehr Rechenleistung auf dem Endbenutzercomputer oder der Transfer Server-Instanz.

Kleine Bereitstellung mit minimalem Investitionsaufwand

Sie können die Anzahl der für Ihre Bereitstellung benötigten ESX-Server reduzieren, wenn Sie die Anzahl der virtuellen Maschinen auf jedem Server erhöhen. Ein ESX 4.1-Server kann bis zu 500 virtuelle Maschinen hosten, wenn die meisten der Maschinen nicht gleichzeitig eingeschaltet werden.

Nutzen Sie die folgenden Empfehlungen, um die von jeder virtuellen Maschine benötigte Bandbreite sowie die Anzahl der E/A-Vorgänge zu verringern sowie die Anzahl der virtuellen Maschinen auf einem ESX-Server zu maximieren.

- Legen Sie eine View-Richtlinie fest, sodass Endbenutzer ihre View-Desktops ausschließlich im lokalen Modus verwenden können. Mit dieser Einstellung bleiben die virtuellen Maschinen im Rechenzentrum gesperrt und ausgeschaltet.
- Legen Sie Richtlinien für den lokalen Modus fest, sodass Endbenutzer keine Desktop-Eincheckvorgänge, -Rollbacks oder -Replikationen durchführen können.
- Legen Sie keine Intervalle für die automatische Replikation fest.
- Konfigurieren Sie die View Connection Server-Einstellungen so, dass für Vorgänge im lokalen Modus weder eine Deduplizierung noch eine Komprimierung verwendet wird. Diese Einstellungen sind möglicherweise nur nützlich, wenn die Datenreplikation lokaler Desktops über ein langsames Netzwerk während einer Zeit erfolgt, zu der die Endbenutzer einen Leistungsabfall auf ihren Clientcomputern bemerken.
- Konfigurieren Sie die View Connection Server-Einstellungen so, dass für Vorgänge im lokalen Modus oder die Bereitstellung kein SSL verwendet wird.
- Verwenden Sie View Composer zum Erstellen von Linked-Clone-Desktops, verwenden Sie jedoch nicht die Funktion für die Neuzusammenstellung. Verwenden Sie stattdessen herkömmliche Mechanismen für Software-Updates, um Patches und Updates direkt auf lokalen Desktops auf Endbenutzercomputern bereitzustellen.
- Wenn die Leistung von View Connection Server durch die Anzahl an lokalen Desktops beeinträchtigt wird, legen Sie ein größeres Taktsignalintervall fest. Der Standardwert lautet 5 Minuten.

Verwalten von View Transfer Server

View Transfer Server ist die View-Komponente zur Unterstützung von Datenübertragungsvorgängen für lokale Desktops.

Grundlegendes zu View Transfer Server

View Transfer Server verwaltet und optimiert Datenübertragungen zwischen dem Rechenzentrum und lokalen Desktops. Für die Unterstützung von Desktops, die View Client with Local Mode unterstützen, wird View Transfer Server benötigt.

View Transfer Server übermittelt in verschiedenen Situationen Daten zwischen dem Remote-Desktop und lokalen Desktops.

- Wenn ein Benutzer einen Desktop ein- oder auscheckt, wird diese Operation von View Manager autorisiert und verwaltet. View Transfer Server überträgt die Dateien zwischen dem Rechenzentrum und dem lokalen Desktop.
- View Transfer Server synchronisiert lokale Desktops mit den entsprechenden Desktops im Rechenzentrum, indem Benutzeränderungen im Rechenzentrum repliziert werden.

  Replikationen finden in Intervallen statt, die Sie in den Richtlinien für den lokalen Modus festlegen. Außerdem können Sie Replikationen in View Administrator starten. Sie können über eine Richtlinie festlegen, dass Benutzer Replikationen über ihre lokalen Desktops initiieren können.
- View Transfer Server verteilt allgemeine Systemdaten vom Rechenzentrum an lokale Clients. View Transfer Server lädt View Composer-Basis-Images aus dem Transfer Server-Repository auf lokale Desktops herunter.

Ein Ereignis, z.B. ein Netzwerkausfall oder das Entfernen von View Transfer Server aus View Manager, kann aktive Datenübertragungen unterbrechen. View Transfer Server setzt die angehaltenen Übertragungen fort, sobald die Komponenten erneut ausgeführt werden.

Hinzufügen von View Transfer Server zu View Manager

View Transfer Server kann zur Übertragung von Dateien und Daten zwischen lokalen Desktops und dem Rechenzentrum mit View Connection Server eingesetzt werden. Damit View Transfer Server diese Aufgaben ausführen kann, müssen Sie den Server zu Ihrer View Manager-Bereitstellung hinzufügen.

Sie können mehrere View Transfer Server-Instanzen zu View Manager hinzufügen. Die View Transfer Server-Instanzen greifen auf ein gemeinsames Transfer Server-Repository zu. Die Übertragungsarbeitslast für die lokalen Desktops, die über eine View Connection Server-Instanz oder von einer Gruppe replizierter View Connection Server-Instanzen verwaltet werden, wird auf diese View Transfer Server-Instanzen verteilt.

Hinweis Beim Hinzufügen von View Transfer Server zu View Manager wird die DRS-Automatisierungsrichtlinie (Distributed Resource Scheduler) auf **[Manual (Manuell)]** eingestellt, wodurch DRS deaktiviert wird.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server auf einer virtuellen Windows Server-Maschine installiert ist.
- Stellen Sie sicher, dass vCenter Server zu View Manager hinzugefügt wurde. Auf der Seite **[View Configuration (View-Konfiguration)] > [Server]** in View Administrator werden vCenter Server-Instanzen angezeigt, die zu View Manager hinzugefügt wurden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Server]** .

2 Klicken Sie im Fenster **[Transfer Servers (Übertragungsserver)]** auf **[Add (Hinzufügen)]** .

3 Wählen Sie im Assistenten zum Hinzufügen von Transfer Server-Instanzen die vCenter Server-Instanz, über welche die virtuelle View Transfer Server-Maschine verwaltet wird und klicken Sie auf **[Next (Weiter)]** .

4 Wählen Sie die virtuelle Maschine, auf der View Transfer Server installiert ist, und klicken Sie auf **[Finish (Fertig stellen)]** .

   View Connection Server konfiguriert die virtuelle Maschine mit vier SCSI-Controllern neu. Durch die Konfiguration mehrerer SCSI-Controller wird die Anzahl an Festplattenübertragungen erhöht, die View Transfer Server gleichzeitig ausführen kann.

Die View Transfer Server-Instanz wird im View Administrator im Fenster **[Transfer Servers (Übertragungsserver)]** angezeigt. Wenn kein Transfer Server-Repository konfiguriert ist, wird der View Transfer Server-Status von **[Pending (Ausstehend)]** in **[Missing Transfer Server Repository (Transfer Server-Repository fehlt)]** geändert. Wenn ein Transfer Server-Repository konfiguriert ist, wird der Status von **[Pending (Ausstehend)]** über **[Initializing Transfer Server repository (Transfer Server-Repository wird initialisiert)]** in **[Ready (Bereit)]** geändert.

Dieser Vorgang kann einige Minuten dauern. Sie können auf die Aktualisierungsschaltfläche in View Administrator klicken, um den aktuellen Status zu überprüfen.

Beim Hinzufügen der View Transfer Server-Instanz zu View Manager wird der Apache-Dienst auf der virtuellen Maschine von View Transfer Server gestartet.

VORSICHT Wenn Ihre virtuelle View Transfer Server-Maschine eine frühere Version aufweist als Hardwareversion 7, muss nach dem Hinzufügen von View Transfer Server zu View Manager die statische IP-Adresse auf der virtuellen View Transfer Server-Maschine konfiguriert werden.

Beim Hinzufügen mehrerer SCSI-Controller zur virtuellen View Transfer Server-Maschine entfernt Windows die statische IP-Adresse und konfiguriert die virtuelle Maschine für die Verwendung von DHCP neu. Nach dem Neustart der virtuellen Maschine muss die statische IP-Adresse erneut in der virtuellen Maschine eingegeben werden.

Entfernen von View Transfer Server aus View Manager

Wenn Sie sämtliche Instanzen von View Transfer Server aus View Manager entfernen, können keine Daten für lokale Desktops ausgecheckt, eingecheckt oder repliziert werden.

Wenn Sie eine View Transfer Server-Instanz entfernen, die zurzeit Übertragungen durchführt, werden die aktiven Übertragungsvorgänge angehalten. Für lokale Desktop-Sitzungen wird der Übertragungsstatus als angehalten angezeigt.

Wenn Sie View Transfer Server beispielsweise beim Auschecken eines Desktops entfernen, wird der Vorgang zum Auschecken angehalten. Der Benutzer kann den angehaltenen Übertragungsvorgang vom Clientcomputer aus fortsetzen.

HINWEIS Sie müssen eine View Transfer Server-Instanz aus View Manager entfernen, bevor Sie die folgenden Vorgänge ausführen:

- Deinstallation oder Upgrade einer View Transfer Server-Instanz
- Ausführen von Wartungsvorgängen auf einer virtuellen View Transfer Server-Maschine in vCenter Server

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie eine View Transfer Server-Instanz aus.

3 Klicken Sie auf **[Remove (Entfernen)]** .

4 Wenn gegenwärtig Übertragungsvorgänge ausgeführt werden, wählen Sie, ob die aktiven Übertragungen abgebrochen werden sollen oder ob diese Aufgabe abgebrochen und View Transfer Server beibehalten werden soll.

5 Klicken Sie auf **[OK]** .

Wenn eine View Transfer Server-Instanz aus View Manager entfernt wird, wird die zugehörige DRS-Automatisierungsrichtlinie auf den Wert zurückgesetzt, auf den sie vor dem Hinzufügen von View Transfer Server zu View Manager festgelegt war.

Verwenden des Wartungsmodus zum Anhalten von Datenübertragungen für lokale Desktops

Wenn Sie eine View Transfer Server-Instanz in den Wartungsmodus versetzen, werden aktive Datenübertragungen angehalten und zukünftige Datenübertragungen für lokale Desktops auf dieser View Transfer Server-Instanz verhindert. Beim Beenden des Wartungsmodus für die View Transfer Server-Instanz können angehaltene Übertragungen vom Client fortgesetzt und neue Übertragungen gestartet werden.

Wenn sich alle View Transfer Server-Instanzen im Wartungsmodus befinden, kann das Transfer Server-Repository migriert werden. Siehe „Migrieren des Transfer Server-Repositorys an einen neuen Speicherort“, auf Seite 306.

Beim Hinzufügen einer View Transfer Server-Instanz im aktiven Modus zu View Manager wird die DRS-Automatisierungsrichtlinie (Distributed Resource Scheduler) auf **[Manual (Manuell)]** eingestellt, wodurch DRS deaktiviert wird. Um eine View Transfer Server-Instanz auf einen anderen ESX-Host oder -Datenspeicher zu migrieren, müssen Sie die Instanz vor Beginn der Migration in den Wartungsmodus versetzen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

2 Wählen Sie eine View Transfer Server-Instanz aus.

3 Klicken Sie auf **[Enter Maintenance Mode (In Wartungsmodus wechseln)]** .

4 Finden gerade Übertragungen statt, müssen Sie entweder die aktiven Übertragungen abbrechen oder warten, bis die aktiven Übertragungen abgeschlossen sind, bevor Sie View Transfer Server in den Wartungsmodus versetzen.

   Wenn Sie aktive Übertragungen abbrechen, wird View Transfer Server umgehend in den Wartungsmodus versetzt.

   Wenn Sie warten, bis aktive Übertragungen abgeschlossen sind, wechselt View Transfer Server in den Status **[Pending (Ausstehend)]** . Wenn die aktuelle Festplattenübertragung abgeschlossen ist, wechselt View Transfer Server in den Wartungsmodus.

   Hinweis Wenn aktive Übertragungen abgeschlossen werden können, ist sichergestellt, dass die aktuelle Festplatte übertragen wird. Virtuelle Maschinen enthalten jedoch mehrere Festplatten. Ein Übertragungsvorgang wie z. B. das Auschecken eines Desktops wird möglicherweise nicht abgeschlossen, wenn keine anderen View Transfer Server-Instanzen verfügbar sind, um weitere Festplatten zu übertragen. Wenn eine View Transfer Server-Instanz aus dem Wartungsmodus genommen wird, können angehaltene Übertragungen abgeschlossen werden.

5 Klicken Sie auf **[OK]** .

Weiter

Wenn Sie bereit sind, den Wartungsmodus für View Transfer Server zu beenden, wählen Sie die View Transfer Server-Instanz aus und klicken Sie auf **[Exit Maintenance Mode (Wartungsmodus beenden)]** . Angehaltene Übertragungen können fortgesetzt und neue Datenübertragungen können gestartet werden.

Verbessern der Übertragungsleistung im WAN auf Windows Server 2003

In einer WAN-Umgebung mit hoher Netzwerklatenz kann die Übertragungsleistung verbessert werden, indem Sie die Größe der TCP-Sende- und -Empfangsfenster erhöhen.

Wenn View Transfer Server auf Windows Server 2008 installiert ist, werden die TCP-Sende- und -Empfangsfenster standardmäßig auf 640 KB erhöht. Diese Werte müssen nicht neu konfiguriert werden.

Wenn View Transfer Server auf Windows Server 2003 installiert ist, müssen Sie manuell Registrierungsschlüssel festlegen, um die Größe der TCP-Sende- und -Empfangsfenster auf 640 KB zu erhöhen.

Voraussetzungen

Stellen Sie sicher, dass View Transfer Server auf Windows Server 2003 installiert ist.

Vorgehensweise

1 Öffnen Sie den Windows-Registrierungs-Editor auf dem Windows Server 2003-Computer, auf dem View Transfer Server installiert ist.

2 Fügen Sie zwei neue Registrierungsschlüssel, **[DefaultSendWindow (Standard-Sendefenster)]** und **[DefaultReceiveWindow (Standard-Empfangsfenster)]** , zu `HKEY_LOCAL_MACHINE, System, CurrentControlSet, Services, AFD, Parameters` hinzu.

3 Setzen Sie die Werte für die Registrierungsschlüssel **[DefaultSendWindow (Standard-Sendefenster)]** und **[DefaultReceiveWindow (Standard-Empfangsfenster)]** auf **`655360`**.

   Sie müssen eine positive Ganzzahl eingeben. Die Werte werden in Byte konfiguriert. Der Schlüsseltyp lautet **[REG_DWORD]** .

4 Starten Sie View Transfer Server neu.

View Transfer Server-Status

View Transfer Server kann verschiedene Betriebs- und Verfügbarkeitsstatus aufweisen. In View Administrator wird der Status von View Transfer Server im Transfer Server-Bereich auf der Seite **[View Configuration (View-Konfiguration)] > [Servers (Server)]** angezeigt.

Tabelle 14-1. View Transfer Server-Statuswerte bei normalen Vorgängen

Status	Beschreibung
Ready (Bereit)	View Transfer Server und das Transfer Server-Repository sind konfiguriert und funktionieren ordnungsgemäß.
Pending (Ausstehend)	View Transfer Server wird zu View Manager hinzugefügt oder beendet den Wartungsmodus. View Connection Server stellt aktiv eine Verbindung zu View Transfer Server her. Nach dem Herstellen der Verbindung wird View Transfer Server in einen Betriebsstatus, z.B. **[Ready (Bereit)]** , versetzt.
Maintenance mode pending (Wartungsmodus ausstehend)	View Transfer Server wechselt in den Wartungsmodus, während auf das Abschließen von aktiven Übertragungen und Paketveröffentlichungsvorgängen gewartet wird.
Maintenance mode (Wartungsmodus)	Aktive Datenübertragungen werden angehalten. Benutzer können keine neuen Übertragungen initiieren. Geplante, ausstehende Übertragungen können nicht ausgeführt werden. View Transfer Server kann keine Pakete im Transfer Server-Repository veröffentlichen.

Tabelle 14-1. View Transfer Server-Statuswerte bei normalen Vorgängen (Fortsetzung)

Status	Beschreibung
Initializing Transfer Server repository (Transfer Server-Repository wird initialisiert)	View Transfer Server initialisiert das Transfer Server-Repository. Wenn bei der Initialisierung des Transfer Server-Repositorys durch View Transfer Server Probleme auftreten, ändert sich der Status in einen Fehlerstatus. Weitere Informationen zur Lösung des Problems finden Sie im Tipp zur Fehlerbehebung des angezeigten Fehlerstatus.
Missing Transfer Server repository (Transfer Server-Repository fehlt)	Es ist kein Transfer Server-Repository in View Manager konfiguriert. Dieser Status weist nicht auf einen Fehler hin, da Sie Übertragungsvorgänge für vollständige virtuelle Maschinen ohne Konfiguration eines Transfer Server-Repositorys ausführen können. Dieser Status verweist jedoch auf einen Fehler, wenn Sie Linked-Clone-Desktops im lokalen Modus verwenden. Sie können für Linked-Clone-Desktops keine Übertragungsvorgänge ausführen, wenn kein Transfer Server-Repository konfiguriert wurde.

View Transfer Server kann in einen Fehlerstatus wechseln, wenn der Dienst nicht verfügbar ist oder nicht normal funktioniert. Weitere Informationen zur Problemlösung finden Sie im Tipp zur Fehlerbehebung des angezeigten Fehlerstatus. Siehe „Fehlerbehebung bei View Transfer Server- und lokalen Desktop-Vorgängen“, auf Seite 332.

Tabelle 14-2. View Transfer Server-Fehlerstatuswerte

Status	Beschreibung
Bad Transfer Server Repository (Ungültiges Transfer Server-Repository)	Das Transfer Server-Repository, mit dem sich View Transfer Server entsprechend der Konfiguration verbindet, unterscheidet sich von dem Transfer Server-Repository, das derzeit in der View Connection Server-Instanz konfiguriert ist.
Repository connection error (Repository-Verbindungsfehler)	View Transfer Server kann keine Verbindung zum Transfer Server-Repository herstellen.
Bad Health Check (Fehler bei Systemzustandsprüfung)	Bei der View Manager-Systemzustandsprüfung für View Transfer Server wurde ein Fehler gemeldet. View Transfer Server ist nicht verfügbar oder funktioniert nicht ordnungsgemäß.
Transfer Server-Repository-Konflikt	Mehrere View Transfer Server-Instanzen sind für die Verbindung mit verschiedenen Transfer Server-Repositorys konfiguriert. Dieser Status kann auftreten, wenn gleichzeitig mehrere View Transfer Server-Instanzen zu View Manager hinzugefügt werden und jede Instanz mit einem anderen Transfer Server-Repository konfiguriert wird.
Web Server down (Webserver nicht aktiv)	Der Apache2.2-Dienst, der das Transfer Server-Repository unterstützt, funktioniert nicht.

Verwalten des Transfer Server-Repositorys

View Transfer Server verwendet das Transfer Server-Repository zum Speichern der View Composer-Image-Dateien, die auf lokale Desktops heruntergeladen werden. Das Transfer Server-Repository ist erforderlich, um Linked-Clone-Desktops zur Ausführung im lokalen Modus auszuchecken.

Verwenden des Transfer Server-Repositorys zum Herunterladen von System-Images

Zur Unterstützung von Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden, speichert das Transfer Server-Repository die View Composer-Basis-Images in einem zugänglichen Datenspeicher. View Manager und View Transfer Server verwenden das Transfer Server-Repository zur Bereitstellung und Aktualisierung lokaler Linked-Clone-Desktops.

Hinweis Wenn Sie keine verknüpften View Composer-Klone im lokalen Modus verwenden, ist die Konfiguration eines Transfer Server-Repositorys nicht erforderlich. Das Transfer Server-Repository wird nicht für Desktops mit vollständigen virtuellen Maschinen verwendet, die im lokalen Modus ausgeführt werden.

Bevor ein Benutzer einen Linked-Clone-Desktop zur Ausführung im lokalen Modus auschecken kann, muss das zugehörige Basis-Image im Transfer Server-Repository veröffentlicht werden.

Wenn Sie eine Image-Datei im Transfer Server-Repository veröffentlichen, speichert View Transfer Server die Dateien als verschlüsselte Pakete. Zur Optimierung der Downloads auf lokale Desktops kann View Transfer Server die Pakete komprimieren.

Wenn ein Benutzer einen Linked-Clone-Desktop zum ersten Mal auscheckt, führt View Transfer Server zwei Vorgänge aus:

- Herunterladen des Basis-Images aus dem Transfer Server-Repository auf den lokalen Computer.
- Herunterladen des Remote-Linked-Clone-Desktops aus dem Rechenzentrum auf den lokalen Computer. Der Desktop umfasst die Deltafestplatte des Linked-Clone-Desktop-Betriebssystems und eine persistente View Composer-Festplatte.

Wenn Sie Linked-Clone-Desktops im Rechenzentrum ausführen, greifen die verknüpften Klone gemeinsam auf ein Basis-Image zu. Beim Ausführen eines Linked-Clone-Desktops im lokalen Modus muss sich eine Kopie des Basis-Images mit dem Linked-Clone-Desktop auf dem lokalen Computer befinden.

Sofern das Basis-Image nicht geändert wird, wird es nur einmal heruntergeladen. Wenn Benutzer ihre Desktops ein- und erneut auschecken, lädt View Transfer Server nicht das Basis-Image, sondern die Deltafestplatten des Linked-Clone-Betriebssystems und die persistenten View Composer-Festplatten herunter.

Wird ein Basis-Image neu zusammengestellt, lädt View Transfer Server das aktualisierte Image aus dem Transfer Server-Repository auf die lokalen Computer herunter, sobald die Benutzer ihre Desktops erneut auschecken. Weitere Informationen finden Sie unter „Neuzusammenstellung von Linked-Clone-Desktops, die im lokalen Modus ausgeführt werden können“, auf Seite 236.

Wichtig Ein Linked-Clone-Desktop, der aus einem Basis-Image erstellt wurden, muss im Rechenzentrum eingecheckt werden, bevor eine Neuzusammenstellung erfolgen kann.

Bestimmen der Größe eines View Composer-Basis-Images

Das Transfer Server-Repository muss eine ausreichende Größe zum Speichern der View Composer-Basis-Images für alle Linked-Clone-Desktops aufweisen, die im lokalen Modus verwendet werden. Um sicherzustellen, dass ein bestimmtes Basis-Image im Transfer Server-Repository gespeichert werden kann, können Sie die ungefähre Größe des Basis-Images bestimmen.

Ein Basis-Image kann eine Größe von mehreren Gigabyte aufweisen.

Die maximale Größe eines Basis-Images entspricht der Summe der Kapazitäten bereitgestellter Festplatten in der übergeordneten virtuellen Maschine. Die tatsächliche Größe des Basis-Images kann unter dem Maximalwert liegen.

Voraussetzungen

Stellen Sie sicher, dass eine übergeordnete virtuelle Maschine zur Erstellung eines Linked-Clone-Desktop-Pools erstellt wurde.

Vorgehensweise

1 Wählen Sie in vSphere Client die übergeordnete virtuelle Maschine aus.

2 Klicken Sie auf **[Edit Settings (Einstellungen bearbeiten)]** .

3 Wählen Sie auf der Registerkarte **[Hardware]** die erste konfigurierte Festplatte.

Wählen Sie zum Beispiel **[Hard Disk 1 (Festplatte 1)]** .

4 Im Fenster **[Disk Provisioning (Festplattenbereitstellung)]** wird die Größe der bereitgestellten Festplatten angezeigt.

5 Wenn die virtuelle Maschine über mehrere Festplatten verfügt, wiederholen Sie die Schritte 3 und 4 für jede zusätzliche Festplatte.

6 Addieren Sie die Größenwerte der bereitgestellten Festplatten, um die Summe zu berechnen.

Konfigurieren des Transfer Server-Repositorys

Im Transfer Server-Repository werden View Composer-basierte Images für Linked-Clone-Desktops gespeichert, die im lokalen Modus ausgeführt werden. Um View Transfer Server Zugriff auf das Transfer Server-Repository zu gewähren, muss dieses in View Manager konfiguriert werden. Wenn Sie keine verknüpften View Composer-Klone im lokalen Modus verwenden, ist die Konfiguration eines Transfer Server-Repositorys nicht erforderlich.

Wenn View Transfer Server in View Manager konfiguriert wird, bevor Sie das Transfer Server-Repository konfigurieren, validiert View Transfer Server während der Konfiguration den Speicherort des Transfer Server-Repositorys.

Wenn Sie mehrere View Transfer Server-Instanzen zu dieser View Manager-Bereitstellung hinzufügen möchten, konfigurieren Sie das Transfer Server-Repository auf einer Netzwerkfreigabe. Andere View Transfer Server-Instanzen können nicht auf ein Transfer Server-Repository zugreifen, das sich auf einem lokalen Laufwerk einer View Transfer Server-Instanz befindet.

Wenn Sie ein Remote-Transfer Server-Repository auf einer Netzwerkfreigabe konfigurieren, müssen Sie eine Benutzer-ID mit Anmeldeinformationen für den Zugriff auf die Netzwerkfreigabe bereitstellen. Als empfohlene Vorgehensweise und zur Erhöhung der Sicherheit sollten Sie den Netzwerkzugriff auf das Transfer Server-Repository auf View-Administratoren beschränken.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server auf einer virtuellen Windows Server-Maschine installiert ist.
- Stellen Sie sicher, dass View Transfer Server zu View Manager hinzugefügt wurde. Siehe „Hinzufügen von View Transfer Server zu View Manager“, auf Seite 297.

  Hinweis Das Hinzufügen von View Transfer Server zu View Manager vor dem Konfigurieren des Transfer Server-Repositorys ist eine empfohlene Vorgehensweise, keine Anforderung.

- Bestimmen Sie die erforderliche Größe des Transfer Server-Repositorys zum Speichern Ihrer View Composer-Basis-Images. Ein Basis-Image kann eine Größe von mehreren Gigabyte aufweisen. Weitere Informationen zum Bestimmen der Größe eines bestimmten Basis-Images finden Sie unter „Bestimmen der Größe eines View Composer-Basis-Images“, auf Seite 302.

Vorgehensweise

1 Konfigurieren Sie einen Pfad und Ordner für das Transfer Server-Repository.

Das Transfer Server-Repository kann sich auf einem lokalen Laufwerk oder auf einer Netzwerkfreigabe befinden.

Option	Aktion
Local Transfer Server repository (Lokales Transfer Server-Repository)	Erstellen Sie auf der virtuellen Maschine, auf der View Transfer Server installiert ist, einen Pfad und Ordner für das Transfer Server-Repository. Beispiel: `C:\TransferRepository\`
Remote Transfer Server repository (Remote-Transfer Server-Repository)	Konfigurieren Sie einen UNC-Pfad für die Netzwerkfreigabe. Beispiel: `\\Server.Domaene.com\TransferRepository\` Alle View Transfer Server-Instanzen, die Sie dieser View Manager-Bereitstellung hinzufügen, müssen über Netzwerkzugriff auf das freigegebene Laufwerk verfügen.

2 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

3 Versetzen Sie alle View Transfer Server-Instanzen in den Wartungsmodus.

a Wählen Sie im Fenster **[Transfer Servers (Übertragungsserver)]** eine View Transfer Server-Instanz aus.

b Klicken Sie auf **[Enter Maintenance Mode (In Wartungsmodus wechseln)]** und anschließend auf **[OK]** .

Der View Transfer Server-Status ändert sich in **[Maintenance mode (Wartungsmodus)]** .

c Wiederholen Sie die Schritte unter Schritt 3a und Schritt 3b für jede Instanz.

Wenn sich alle View Transfer Server-Instanzen im Wartungsmodus befinden, werden alle aktuellen Übertragungsvorgänge gestoppt.

4 Klicken Sie im Fenster **[Transfer Servers (Übertragungsserver)]** neben dem Transfer Server-Repository auf **[None Configured (Nicht konfiguriert)]** .

5 Klicken Sie auf der Seite für das Transfer Server-Repository im Bereich **[General (Allgemein)]** auf **[Edit (Bearbeiten)]** .

6 Geben Sie den Speicherort des Transfer Server-Repositorys und weitere Informationen ein.

Option	Beschreibung
Netzwerkfreigabe	■ **[Path (Pfad)]** . Geben Sie den konfigurierten UNC-Pfad ein. ■ **[Username (Benutzername)]** . Geben Sie die Benutzer-ID eines Administrators ein, der über Anmeldeinformationen zum Zugriff auf die Netzwerkfreigabe verfügt. ■ **[Password (Kennwort)]** . Geben Sie das Administratorkennwort ein. ■ **[Domain (Domäne)]** . Geben Sie den Domänennamen der Netzwerkfreigabe im NetBIOS-Format ein. Verwenden Sie nicht das Suffix `.com`.
Lokales Dateisystem	Geben Sie den Pfad ein, den Sie auf der lokalen virtuellen Maschine für View Transfer Server konfiguriert haben.

7 Klicken Sie auf **[OK]** .

Wenn der Netzwerkpfad oder das lokale Laufwerk für das Repository falsch angegeben wurden, zeigt das Dialogfeld zum Bearbeiten des Transfer Server-Repositorys eine Fehlermeldung an, und der Speicherort kann nicht konfiguriert werden. Sie müssen einen gültigen Speicherort eingeben.

8 Wählen Sie auf der Seite **[View Configuration (View-Konfiguration)] > [Servers (Server)]** die View Transfer Server-Instanz und klicken Sie auf **[Exit Maintenance Mode (Wartungsmodus beenden)]** .

Der View Transfer Server-Status ändert sich in **[Ready (Bereit)]** .

Veröffentlichen von Paketdateien im Transfer Server-Repository

Bevor ein Benutzer einen Linked-Clone-Desktop auschecken kann, muss das zugehörige View Composer-Basis-Image als Paket im Transfer Server-Repository veröffentlicht werden.

Wenn ein Benutzer einen Linked-Clone-Desktop auscheckt, lädt die View Transfer Server-Instanz die Basis-Image-Paketdateien des Klons aus dem Transfer Server-Repository auf den lokalen Computer herunter.

Pakete können in View Administrator auf der Seite **[Transfer Server repository (Transfer Server-Repository)]** veröffentlicht werden. Pakete können zudem beim Erstellen eines Linked-Clone-Pools veröffentlicht werden. Nach dem Erstellen eines Pools können Pakete auch über die Seite des jeweiligen Pools veröffentlicht werden, indem Sie die Option **[View Composer] > [Publish (Veröffentlichen)]** verwenden.

Voraussetzungen

- Stellen Sie sicher, dass in View Manager eine View Transfer Server-Instanz konfiguriert ist. Siehe „Hinzufügen von View Transfer Server zu View Manager“, auf Seite 297.
- Stellen Sie sicher, dass das Transfer Server-Repository in View Manager konfiguriert ist. Siehe „Konfigurieren des Transfer Server-Repositorys“, auf Seite 303.
- Stellen Sie sicher, dass das Transfer Server-Repository groß genug ist, um das Basis-Image (dessen Größe mehrere Gigabyte betragen kann) zu speichern. Das Basis-Image muss im Repository gespeichert werden können, bevor die Paketdateien komprimiert werden. Siehe „Bestimmen der Größe eines View Composer-Basis-Images“, auf Seite 302.
- Stellen Sie sicher, dass ein Linked-Clone-Desktop-Pool zur Verwendung im lokalen Modus erstellt wurde.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

2 Klicken Sie auf **[Publish (Veröffentlichen)]** .

3 Wählen Sie ein View Composer-Basis-Image aus der Liste aus und klicken Sie auf **[Next (Weiter)]** .

4 Klicken Sie auf **[Finish (Fertig stellen)]** .

Das Paket wird im Fensterbereich **[Contents (Inhalte)]** auf der Seite **[Transfer Server Repository (Transfer Server-Repository)]** angezeigt. Der Paketstatus ändert sich von **[Initializing (Wird initialisiert)]** über **[Publishing (Wird veröffentlicht)]** in **[Published (Veröffentlicht)]** .

Der Veröffentlichungsvorgang kann einige Zeit in Anspruch nehmen. Klicken Sie auf das Aktualisierungssymbol auf der Transfer-Repository-Seite, um den Fortschritt des Vorgangs in Prozent anzuzeigen.

View Transfer Server kann das veröffentlichte View Composer-Basis-Image auf lokale Desktops herunterladen.

Löschen einer Paketdatei aus dem Transfer Server-Repository

View Transfer Server speichert View Composer-Basis-Images als Paketdateien im Transfer Server-Repository. Wenn diese Dateien veraltet sind oder nicht mehr verwendet werden, können Sie die Pakete aus dem Transfer Server-Repository löschen.

Sie können eine Paketdatei auch dann löschen, wenn Linked-Clone-Desktops weiterhin das Basis-Image verwenden, über das die Paketdatei veröffentlicht wurde. Nach dem Löschen der Paketdatei können diese Desktops nicht ausgecheckt werden.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server in View Manager konfiguriert ist. Siehe „Hinzufügen von View Transfer Server zu View Manager“, auf Seite 297.
- Stellen Sie sicher, dass ein Transfer Server-Repository konfiguriert ist. Siehe „Konfigurieren des Transfer Server-Repositorys“, auf Seite 303.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

2 Wählen Sie im Fenster **[Contents (Inhalt)]** eine Paketdatei aus.

3 Klicken Sie auf **[Remove (Entfernen)]** .

Wenn Linked-Clone-Desktops das Basis-Image verwenden, über das die ausgewählte Paketdatei veröffentlicht wurde, wird eine Warnmeldung angezeigt. Sie können den Vorgang zum Entfernen des Pakets abbrechen oder fortsetzen.

4 Klicken Sie auf **[OK]** .

Das Paket wechselt in den Status **[Pending Delete (Löschen steht aus)]** und wird gelöscht.

Migrieren des Transfer Server-Repositorys an einen neuen Speicherort

Sie können das Transfer Server-Repository an einen neuen Speicherort migrieren, wenn der Speicherplatz auf dem aktuellen Festplattenlaufwerk knapp wird.

Alle View Transfer Server-Instanzen, die mit einem View Connection Server verknüpft sind, müssen sich im Wartungsmodus befinden, bevor Sie das Transfer Server-Repository migrieren können.

Wenn Sie über mehrere View Transfer Server-Instanzen verfügen, migrieren Sie das Transfer Server-Repository auf ein im Netzwerk freigegebenes Laufwerk. Andere View Transfer Server-Instanzen können nicht auf ein Transfer Server-Repository zugreifen, das sich auf einem lokalen Laufwerk einer View Transfer Server-Instanz befindet.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server installiert und konfiguriert wurde. Siehe „Hinzufügen von View Transfer Server zu View Manager“, auf Seite 297.
- Veröffentlichen Sie keine Pakete im Transfer Server-Repository, während Sie das Repository migrieren. Wenn ein Paket im aktuellen Repository veröffentlicht wird, nachdem Sie mit dem Kopieren der Repositorydateien an den neuen Speicherort begonnen haben, wird das Paket möglicherweise nicht an den neuen Speicherort kopiert.

  Zur Erzwingung dieser Vorbedingung können Sie View Transfer Server in den Wartungsmodus versetzen, bevor Sie das Repository manuell kopieren. Dieser Ansatz verlängert jedoch die Ausfallzeit für Datenübertragungen, während die Repositorydateien kopiert werden.

  Kopieren Sie stattdessen die Repositorydateien, bevor Sie View Transfer Server in den Wartungsmodus versetzen. Dieser Ansatz minimiert die Zeit, in der View Transfer Server nicht verfügbar ist.

Vorgehensweise

1 Konfigurieren Sie einen lokalen oder Remote-Zielordner, in den Sie das Transfer Server-Repository migrieren.

Option	Aufgabe
Local Transfer Server repository (Lokales Transfer Server-Repository)	Erstellen Sie auf der virtuellen Maschine, auf der View Transfer Server installiert ist, einen Pfad und Ordner für das Transfer Server-Repository. Beispiel: `C:\TransferRepository\`
Remote Transfer Server repository (Remote-Transfer Server-Repository)	Konfigurieren Sie einen UNC-Pfad für die Netzwerkfreigabe. Beispiel: `\\server.domain.com\TransferRepository\` Alle View Transfer Server-Instanzen, die Sie dieser View Manager-Bereitstellung hinzufügen, müssen über Netzwerkzugriff auf das freigegebene Laufwerk verfügen.

2 Kopieren Sie das Stammverzeichnis des Transfer Server-Repositorys manuell an den Zielspeicherort.

Sie müssen das gesamte Stammverzeichnis kopieren, nicht lediglich die Paketdateien, die sich unterhalb des Stammverzeichnisses befinden.

3 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

4 Versetzen Sie alle View Transfer Server-Instanzen in den Wartungsmodus.

a Wählen Sie im Fenster **[Transfer Servers (Übertragungsserver)]** eine View Transfer Server-Instanz aus.

b Klicken Sie auf **[Enter Maintenance Mode (In Wartungsmodus wechseln)]** und anschließend auf **[OK]** .

Der View Transfer Server-Status ändert sich in **[Maintenance (Wartung)]** .

c Wiederholen Sie diese Schritte für jede Instanz.

Wenn sich alle View Transfer Server-Instanzen im Wartungsmodus befinden, werden alle aktuellen Übertragungsvorgänge gestoppt.

5 Klicken Sie im Bereich **[Transfer Servers (Übertragungsserver)]** auf den Pfad für das Transfer Server-Repository.

Beispiel: `C:\TransferRepository`.

6 Klicken Sie auf der Seite für das Transfer Server-Repository im Bereich **[General (Allgemein)]** auf **[Edit (Bearbeiten)]** .

7 Geben Sie den Zielspeicherort und weitere Informationen zum Transfer Server-Repository ein.

Option	Beschreibung
Netzwerkfreigabe	■ **[Path (Pfad)]** . Geben Sie den konfigurierten UNC-Pfad ein. ■ **[Username (Benutzername)]** . Geben Sie die Benutzer-ID eines Administrators ein, der über Anmeldeinformationen zum Zugriff auf die Netzwerkfreigabe verfügt. ■ **[Password (Kennwort)]** . Geben Sie das Administratorkennwort ein. ■ **[Domain (Domäne)]** . Geben Sie den Domänennamen der Netzwerkfreigabe im NetBIOS-Format ein. Verwenden Sie nicht das Suffix `.com`.
Lokales Dateisystem	Geben Sie den Pfad ein, den Sie auf der lokalen virtuellen Maschine für View Transfer Server konfiguriert haben.

8 Klicken Sie auf **[OK]** .

9 Wählen Sie auf der Seite **[View Configuration (View-Konfiguration)] > [Servers (Server)]** jede View Transfer Server-Instanz, klicken Sie auf **[Exit Maintenance Mode (Wartungsmodus beenden)]** und anschließend auf **[OK]** .

Der View Transfer Server-Status ändert sich in **[Ready (Bereit)]** .

10 (Optional) Löschen Sie die Paketdateien manuell aus dem ursprünglichen Transfer Server-Repository-Ordner.

Wiederherstellen eines beschädigten Transfer Server-Repository-Ordners

Wenn der im Netzwerk freigegebene Ordner oder der lokale Ordner, in dem das Transfer Server-Repository konfiguriert ist, beschädigt wird, müssen Sie das Transfer Server-Repository in einem nicht beschädigten Ordner neu erstellen.

Diese Situation tritt ein, wenn kein Zugriff auf die Netzwerkfreigabe oder das lokale Laufwerk möglich ist und Sie nicht auf die Transfer Server-Paketdateien zugreifen können, die in dem konfigurierten Ordner gespeichert sind. In diesem Fall können Sie die Paketdateien nicht manuell aus dem beschädigten Ordner in einen neuen Ordner kopieren.

Voraussetzungen

- Machen Sie sich mit der Konfiguration eines Transfer Server-Repositorys vertraut. Siehe „Konfigurieren des Transfer Server-Repositorys“, auf Seite 303.
- Machen Sie sich mit dem Entfernen und Hinzufügen von View Transfer Server in View Manager und dem Versetzen von View Transfer Server in den Wartungsmodus vertraut. Siehe „Verwalten von View Transfer Server“, auf Seite 297.
- Machen Sie sich mit dem Veröffentlichen und Löschen von Paketen im Transfer Server-Repository vertraut. Siehe „Veröffentlichen von Paketdateien im Transfer Server-Repository“, auf Seite 305 und „Löschen einer Paketdatei aus dem Transfer Server-Repository“, auf Seite 305.

Vorgehensweise

1 Entfernen Sie alle View Transfer Server-Instanzen aus View Manager.

Wenn alle View Transfer Server-Instanzen entfernt wurden, löscht View Manager die Konfiguration des Transfer Server-Repositorys (einschließlich des Pfads und der zugehörigen Informationen).

2 Konfigurieren Sie einen neuen Pfad und einen neuen Ordner für eine Netzwerkfreigabe oder ein lokales Laufwerk.

Führen Sie dieselben Schritte wie beim Erstellen eines neuen Transfer Server-Repositorys aus.

3 Fügen Sie die View Transfer Server-Instanzen zu View Manager hinzu.

4 Versetzen Sie die View Transfer Server-Instanzen in den Wartungsmodus.

5 Konfigurieren Sie das Transfer Server-Repository in View Manager und geben Sie die neue Netzwerkfreigabe oder den neuen lokalen Pfad an.

View Transfer Server validiert den neuen Pfad für das Transfer Server-Repository. Der Status der einzelnen Pakete lautet **[Missing Package (Fehlendes Paket)]** .

6 Versetzen Sie die einzelnen View Transfer Server-Instanzen erneut in den Status **[Ready (Bereit)]** , indem Sie den Wartungsmodus beenden.

7 Löschen Sie die abgelösten Pakete aus dem Transfer Server-Repository.

8 Veröffentlichen Sie die Pakete im Transfer Server-Repository neu.

Verwenden Sie die ursprünglichen übergeordneten virtuellen Maschinen und Snapshots zur Veröffentlichung der View Composer-Basis-Images als Pakete im Repository.

Verwalten von Datenübertragungen

Sie können Richtlinien zur Konfiguration von Replikationen und Optimierung von Übertragungsvorgängen festlegen. Darüber hinaus können Sie zwischen geplanten Replikationen Replikationsanforderungen initiieren. Um die lokal ausgecheckte Version zu verwerfen, kann bei Bedarf ein Rollback für einen Desktop ausgeführt werden.

Um die Integrität lokaler Desktop-Daten beizubehalten, werden Replikationsvorgänge als Sequenz ausgeführt.

Bei jeder Replikation werden Daten von einem Snapshot übertragen, der beim Start der Replikation für den lokalen Desktop erstellt wird. Daher stellt jede Replikation einen anderen Status des lokalen Desktops dar.

Wenn Sie eine Replikation initiieren oder wenn der Start einer Replikation geplant ist, wird die Anforderung ausgeführt, sobald der Clientcomputer das Rechenzentrum kontaktiert. View Client with Local Mode erstellt einen Snapshot und startet die Replikation.

View verwaltet jeweils nur eine ausstehende Replikation.

Hinweis Zu Beginn und am Ende eines Replikationsvorgangs ist die Desktop-Leistung möglicherweise für wenige Sekunden beeinträchtigt, während ein lokaler Snapshot erstellt oder aktualisiert wird.

- Festlegen von Replikationsrichtlinien auf Seite 309

  Bei der Replikation werden lokale Desktops mit den zugehörigen Remote-Desktops synchronisiert, indem von den Benutzern generierte Änderungen an das Rechenzentrum gesendet werden. Sie können Richtlinien festlegen, um die Häufigkeit der Replikation zu konfigurieren, das Anhalten von Replikationen durch die Benutzer zuzulassen und den Typ der Linked-Clone-Festplatte für die Replikation auszuwählen.

- Initiieren von Replikationen lokaler Desktops auf Seite 310

  Sie können Replikationen für Desktops initiieren, die im lokalen Modus ausgeführt werden. Durch Ihre Anforderung kann vor der nächsten geplanten Replikation ein Replikationsvorgang gestartet werden. Wenn die Clientrichtlinie dies zulässt, kann ein Endbenutzer, der einen lokalen Desktop ausgecheckt hat, in View Client auch eine Replikation für den Desktop initiieren.

- Rollback eines lokal ausgecheckten Desktops auf Seite 311

  Wenn ein Endbenutzer einen Laptop verliert, auf dem sich ein lokaler Desktop befindet, oder wenn die Festplatte beschädigt wird, können Sie ein Rollback des View-Desktops durchführen, damit der Endbenutzer den Desktop auf einem anderen Computer auschecken kann. Wenn die Clientrichtlinie dies zulässt, kann ein Endbenutzer, der einen lokalen Desktop ausgecheckt hat, in View Client auch ein Rollback für den Desktop durchführen.

- Löschen eines lokalen Desktops auf Seite 312

  Wen Sie ein Rollback für einen lokalen Desktop durchführen oder View Client deinstallieren, werden die Dateien des lokalen Desktops auf diesem Clientcomputer weder gelöscht noch bereinigt. Zum Entfernen eines lokalen Desktops müssen alle zugehörigen Dateien manuell gelöscht werden.

Festlegen von Replikationsrichtlinien

Bei der Replikation werden lokale Desktops mit den zugehörigen Remote-Desktops synchronisiert, indem von den Benutzern generierte Änderungen an das Rechenzentrum gesendet werden. Sie können Richtlinien festlegen, um die Häufigkeit der Replikation zu konfigurieren, das Anhalten von Replikationen durch die Benutzer zuzulassen und den Typ der Linked-Clone-Festplatte für die Replikation auszuwählen.

Replikationsoptionen werden über Richtlinien für den lokalen Modus konfiguriert. Eine Beschreibung finden Sie unter „Richtlinien für den lokalen Modus“, auf Seite 166.

Voraussetzungen

Legen Sie fest, ob diese Richtlinien global, für einzelne Desktop-Pools oder für einzelne Benutzer festgelegt werden. Weitere Informationen finden Sie unter „Festlegen von Richtlinien in View Administrator“, auf Seite 163.

Vorgehensweise

- Legen Sie einen Wert für **[Target replication frequency (Zielreplikationshäufigkeit)]** fest.

  Über diese Richtlinie wird das Intervall in Tagen, Stunden oder Minuten zwischen dem Start einer Replikation und dem Start der nächsten Replikation angegeben. Bei Auswahl von **[No replication (Keine Replikation)]** sind keine geplanten Replikationen zulässig.

  Durch die Richtlinie **[No replication (Keine Replikation)]** werden explizite Replikationsanforderungen nicht verhindert. Wenn die Richtlinie **[User initiated replication (Vom Benutzer initiierte Replikation)]** auf **[Allow (Zulassen)]** gesetzt ist, können Sie Replikationen in View Administrator initiieren und Benutzer können Replikationen anfordern.

  Wenn eine Replikation länger dauert als das in der Richtlinie **[Target replication frequency (Zielreplikationshäufigkeit)]** angegebene Intervall, wird die nächste geplante Replikation gestartet, sobald die vorherige Replikation abgeschlossen ist. Die vorherige Replikation wird durch die ausstehende Replikation nicht beendet.

  Beispiel: In der Richtlinie **[Target replication frequency (Zielreplikationshäufigkeit)]** ist als Intervall ein Tag festgelegt. Eine Replikation kann beispielsweise um 12:00 Uhr am Dienstag beginnen. Wenn der Clientcomputer vom Netzwerk getrennt ist, kann die Replikation länger als 24 Stunden in Anspruch nehmen. Am Mittwoch um 12:00 Uhr startet View Client with Local Mode die nächste Replikationsanforderung. Nach Abschluss der vorherigen Replikation erstellt View Client with Local Mode einen Snapshot und startet die ausstehende Replikation.

- Legen Sie **[User deferred replication (Vom Benutzer verzögerte Replikation)]** fest.

  Diese Richtlinie ermöglicht es einem Benutzer, eine ausgeführte Replikation anzuhalten. Die Replikation wird nicht fortgesetzt und neue Replikationen werden erst nach Ablauf des Verzögerungszeitraums gestartet. Der Verzögerungszeitraum beträgt zwei Stunden.

- Legen Sie **[Disks replicated (Replizierte Festplatten)]** fest.

  Über diese Richtlinie wird festgelegt, ob nur persistente View Composer-Festplatten, Betriebssystemfestplatten oder sowohl Betriebssystemfestplatten als auch persistente Festplatten repliziert werden. Diese Richtlinie gilt nur für Linked-Clone-Desktops.

  Sie wird beim Auschecken eines Desktops festgelegt. Änderungen an dieser Richtlinie werden wirksam, nachdem der Desktop erneut ausgecheckt wurde.

- Legen Sie **[User initiated replication (Vom Benutzer initiierte Replikation)]** fest.

  Über diese Richtlinie wird zugelassen, dass Benutzer eine Replikation von einem lokalen Desktop anfordern.

Initiieren von Replikationen lokaler Desktops

Sie können Replikationen für Desktops initiieren, die im lokalen Modus ausgeführt werden. Durch Ihre Anforderung kann vor der nächsten geplanten Replikation ein Replikationsvorgang gestartet werden. Wenn die Clientrichtlinie dies zulässt, kann ein Endbenutzer, der einen lokalen Desktop ausgecheckt hat, in View Client auch eine Replikation für den Desktop initiieren.

Wenn Sie eine Replikation initiieren, während durch View Client with Local Mode bereits Daten repliziert werden, wird der von Ihnen angeforderte Replikationsvorgang gestartet, sobald die vorherige Replikation abgeschlossen ist. Die vorherige Replikation wird durch die ausstehende Replikation nicht abgebrochen.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Monitoring (Überwachung)] > [Local Sessions (Lokale Sitzungen)]** .

2 Wählen Sie lokale Desktops aus.

3 Klicken Sie auf **[Initiate Replication (Replikation initiieren)]** .

4 Wählen Sie, ob die Replikation bei der nächsten Verbindungsherstellung zwischen dem lokalen Desktop und dem Rechenzentrum gestartet werden soll.

Option	Beschreibung
Ja.	Die Replikation wird gestartet, sobald View Client ausgeführt wird und der Desktop das Rechenzentrum kontaktiert.
No (Nein)	Die Replikationsanforderung wird abgebrochen. Wenn Sie zuvor eine Replikation angefordert haben und diese noch nicht gestartet wurde, können Sie die ausstehende Replikation durch Auswahl von **[No (Nein)]** abbrechen.

5 Klicken Sie auf **[OK]** .

Die Replikation wird gestartet, sobald View Client ausgeführt wird und der Clientcomputer das Rechenzentrum kontaktiert. Wenn bereits eine Replikation ausgeführt wird, wird der von Ihnen angeforderte Replikationsvorgang gestartet, sobald die vorherige Replikation abgeschlossen ist.

Weiter

Wenn Sie die Replikation initiiert haben, um den Desktop ohne Endbenutzerinteraktion erneut einzuchecken, können Sie nach Abschluss der Replikation ein Rollback für den lokalen Desktop ausführen. Siehe „Rollback eines lokal ausgecheckten Desktops“, auf Seite 311.

Rollback eines lokal ausgecheckten Desktops

Wenn ein Endbenutzer einen Laptop verliert, auf dem sich ein lokaler Desktop befindet, oder wenn die Festplatte beschädigt wird, können Sie ein Rollback des View-Desktops durchführen, damit der Endbenutzer den Desktop auf einem anderen Computer auschecken kann. Wenn die Clientrichtlinie dies zulässt, kann ein Endbenutzer, der einen lokalen Desktop ausgecheckt hat, in View Client auch ein Rollback für den Desktop durchführen.

Wenn ein Administrator einen Rollback-Vorgang startet, führt der Client eine der folgenden Aktionen aus:

- Wenn der Benutzer am ausgecheckten Desktop angemeldet ist, wird die Sitzung beendet, sobald View Client eine Benachrichtigung empfängt. Der Benutzer kann sich nicht länger am ausgecheckten Desktop anmelden.
- Ist der Benutzer nicht angemeldet, werden nachfolgende Verbindungsversuche an die Online-Kopie des Desktops umgeleitet. Um die Arbeit im lokalen Modus fortzusetzen, muss der Benutzer den Desktop nun vom Server auschecken.

Voraussetzungen

Wenn ein Administrator die aktuellsten Daten des lokalen Desktops beibehalten möchte, führen Sie eine Replikation durch. Siehe „Initiieren von Replikationen lokaler Desktops“, auf Seite 310.

Wichtig Wenn Sie eine Replikation durchführen, müssen Sie den Abschluss der Replikation abwarten, bevor Sie ein Rollback einleiten können. Rollback-Vorgänge werden nicht durch Durchführung nach anderen Vorgängen in die Warteschlange eingereiht. Um zu ermitteln, ob eine Replikation abgeschlossen wurde, klicken Sie in View Administrator auf **[Monitoring (Überwachung)] > [Local Sessions (Lokale Sitzungen)]** und überprüfen Sie die Uhrzeit des Abschlusses der letzten Replikation.

Vorgehensweise

- Wählen Sie die Option **[Rollback]** .

Option	Aktion
View Administrator-Benutzer	Wählen Sie in View Administrator **[Monitoring (Überwachung)]** > **[Local Sessions (Lokale Sitzungen)]** , wählen Sie den Desktop aus und klicken Sie auf **[Rollback]** .
Endbenutzer	Wenn Sie als Benutzer für den Desktop berechtigt sind, klicken Sie in View Client mit der rechten Maustaste in der Liste der verfügbaren Desktops auf den Desktop und wählen Sie **[Rollback]** . Die Option **[Rollback]** ist nur verfügbar, wenn die Client-Desktop-Richtlinie diesen Vorgang zulässt.

Die ausgecheckte Version des Desktops wird verworfen. Ein Benutzer muss die Online-Version erneut auschecken, um den Desktop im lokalen Modus zu verwenden.

Weiter

Zur Bereinigung der Dateien auf dem Endbenutzercomputer muss der Endbenutzer das Verzeichnis im lokalen Modus für diesen Desktop löschen. Siehe „Löschen eines lokalen Desktops“, auf Seite 312.

Informationen zum Auschecken eines View-Desktops für die Verwendung im lokalen Modus finden Sie im Dokument *Installation von VMware View*.

Löschen eines lokalen Desktops

Wen Sie ein Rollback für einen lokalen Desktop durchführen oder View Client deinstallieren, werden die Dateien des lokalen Desktops auf diesem Clientcomputer weder gelöscht noch bereinigt. Zum Entfernen eines lokalen Desktops müssen alle zugehörigen Dateien manuell gelöscht werden.

Voraussetzungen

Stellen Sie sicher, dass der lokale Desktop nicht länger ausgecheckt ist. Wenn der lokale Desktop Daten enthält, die nicht auf den View-Desktop repliziert wurden, der sich im Rechenzentrum befindet, bitten Sie den Endbenutzer darum, den Desktop einzuchecken. Wenn ein Einchecken des Desktops nicht möglich ist, verwenden Sie View Administrator, um die Daten zu replizieren. Siehe „Initiieren von Replikationen lokaler Desktops“, auf Seite 310.

Vorgehensweise

- Wählen Sie auf dem Clientcomputer den Ordner aus, der die Dateien des zu löschenden lokalen Desktops enthält. Löschen Sie den Ordner.

  Der Ordner befindet sich im Auscheckverzeichnis des lokalen Desktops. Wenn Sie beim ersten Herunterladen des Desktops nicht auf **[Options (Optionen)]** geklickt und das Verzeichnis zur Speicherung der lokalen Desktops geändert haben, werden lokale Desktops im Standardverzeichnis für das Auschecken gespeichert.

Desktop-Betriebssystem	Standardverzeichnis für das Auschecken
Standardverzeichnis unter Windows 7 und Windows Vista	`C:\Benutzer\`*`Benutzername`*`\AppData\Local\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*
Standardverzeichnis unter Windows XP	`C:\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*

  Das Verzeichnis `AppData` ist in Windows 7 ein versteckter Ordner. Sie müssen möglicherweise diesen versteckten Ordner anzeigen, um zu den Dateien des lokalen Desktops zu navigieren.

Konfigurieren von Sicherheits- und Optimierungseinstellungen für lokale Desktop-Vorgänge

Sie können eine getunnelte Kommunikation und die SSL-Verschlüsselung für lokale Desktop-Vorgänge konfigurieren. Darüber hinaus können Sie Datenübertragungen zwischen den lokalen Computern und dem Rechenzentrum optimieren.

Diese Einstellungen sind spezifisch für eine einzelne View Connection Server-Instanz. Möglicherweise möchten Sie diese Einstellungen auf einer Instanz aktivieren, auf die Benutzer des lokalen Desktops über das Internet zugreifen, die Einstellungen auf einer dedizierten Instanz für interne Benutzer, die keine lokalen Desktops verwenden, jedoch deaktivieren.

Voraussetzungen

- Machen Sie sich mit den Einstellungen für SSL und die getunnelte Kommunikation für lokale Desktop-Vorgänge vertraut. Siehe „Festlegen von Sicherheitsoptionen für lokale Desktop-Vorgänge“, auf Seite 314.
- Machen Sie sich mit der Verwendung von Deduplizierung und Komprimierung zum Optimieren von Datenübertragungen im Netzwerk vertraut. Siehe „Optimieren der Datenübertragung zwischen Hostcomputern lokaler Desktops und dem Rechenzentrum“, auf Seite 313.

Vorgehensweise

1. Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .
2. Wählen Sie im Fenster mit den View-Servern eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .
3. Wählen Sie Sicherheits- und Optimierungseinstellungen für Datenübertragungen und lokale Desktop-Vorgänge aus.

Optimieren der Datenübertragung zwischen Hostcomputern lokaler Desktops und dem Rechenzentrum

Sie können die Datenmenge reduzieren, die während Übertragungsvorgängen zwischen den Clientcomputern, auf denen lokale Desktops gehostet werden, und dem Rechenzentrum übermittelt wird. Zur Optimierung von Datenübertragungen werden die Deduplizierung und die Komprimierung verwendet.

Tabelle 14-3 zeigt die Deduplizierungs- und Komprimierungseinstellungen für Datenübertragungen.

Übertragungsvorgänge umfassen das Ein- und Auschecken von Desktops, Replizieren von Daten der lokalen Desktops im Rechenzentrum und Herunterladen von System-Images auf lokale Desktops.

Sie können die Auswirkung von Deduplizierung und Komprimierung auf Datenübertragungen ermitteln, indem Sie die View Client with Local Mode-Protokolle überprüfen. Siehe „Ermitteln der Auswirkung von Deduplizierung und Komprimierung auf Datenübertragungen“, auf Seite 316.

Tabelle 14-3. Deduplizierungs- und Komprimierungseinstellungen für Datenübertragungen

Einstellung	Beschreibung
[Use deduplication for Local Mode operations (Deduplizierung für Vorgänge im lokalen Modus verwenden)]	Diese Einstellung verhindert, dass redundante Daten von Clientcomputern an das Rechenzentrum gesendet werden. Die Deduplizierung wird für Übertragungen vom Clientcomputer an das Rechenzentrum (einschließlich Replikationen und Vorgänge zum Einchecken von Desktops) verwendet. Bei ausgecheckten Desktops erfolgt keine Deduplizierung. Bei Verwendung der Deduplizierung ermittelt der Clientcomputer identische Datenblöcke und sendet einen Verweis zum ursprünglichen Block, anstatt den gesamten Block erneut zu senden. Da bei der Deduplizierung Netzwerkbandbreite eingespart wird, ist dieser Prozess bei langsamen Netzwerken sehr nützlich. Die Ermittlung identischer Datenblöcke kann jedoch zu einer erhöhten CPU-Arbeitslast auf dem Clientcomputer und das Lesen duplizierter Blöcke von der Festplatte zu einer erhöhten E/A-Arbeitslast auf der View Transfer Server-Instanz führen. In schnellen Netzwerken ist es möglicherweise effizienter, die Deduplizierung zu deaktivieren. Standardmäßig wird die Deduplizierung nicht verwendet.
[Use compression for Local Mode operations (Komprimierung für Vorgänge im lokalen Modus verwenden)]	Mit dieser Einstellung werden die System-Image- und Desktop-Dateien vor der Übertragung im Netzwerk komprimiert. Wie die Deduplizierung führt die Komprimierung zu Bandbreiteneinsparungen und schnelleren Übertragungen in langsamen Netzwerken. View Transfer Server benötigt zum Komprimieren der Dateien jedoch zusätzliche Computing-Ressourcen. Bei der Entscheidung für oder gegen die Komprimierung müssen die Vorteile bei der Netzwerkleistung und die Server-Computing-Kosten gegeneinander abgewogen werden. Standardmäßig wird die Komprimierung nicht verwendet.

Festlegen von Sicherheitsoptionen für lokale Desktop-Vorgänge

Sie können die Sicherheitsebene für Übertragungsvorgänge festlegen, indem Sie die SSL-Verschlüsselung und Tunnelverbindungen zwischen den Clientcomputern, auf denen lokale Desktops gehostet werden, und dem Rechenzentrum verwenden.

Tabelle 14-4 zeigt die Sicherheitseinstellungen für lokale Desktop-Vorgänge.

Ohne SSL oder Tunnelverbindungen steigt die Datenübertragungsgeschwindigkeit, die Sicherheit der Datenkommunikation wird jedoch reduziert.

Die SSL-Einstellungen wirken sich nicht auf lokale Daten auf Clientcomputern aus, die immer verschlüsselt werden.

Die lokale Datenfestplatte auf Clientsystemen wird standardmäßig mit AES-128 verschlüsselt. Die Verschlüsselungsschlüssel werden verschlüsselt auf dem Clientsystem gespeichert. Der zu diesem Zweck verwendete Schlüssel wird von einem Hash-Wert der Benutzeranmeldeinformationen (Benutzername und Kennwort oder Smartcard und PIN) abgeleitet. Serverseitig wird der Schlüssel in View LDAP gespeichert. Zum Schützen der in LDAP gespeicherten Verschlüsselungsschlüssel für den lokalen Modus sind dieselben Sicherheitsmaßnahmen zu ergreifen wie zum Schützen von View LDAP auf dem Server.

Tabelle 14-4. Verwenden von sicheren Tunnelverbindungen und SSL für lokale Desktop-Vorgänge

Einstellung	Beschreibung
[Use secure tunnel connection for Local Mode operations (Sichere Tunnelverbindung für Vorgänge im lokalen Modus verwenden)]	Lokale Desktops verwenden Tunnelverbindungen. Netzwerkdatenverkehr wird durch View Connection Server oder einen Sicherheitsserver (sofern konfiguriert) geleitet. Wenn Sie diese Einstellung nicht verwenden, werden Datenübertragungen direkt zwischen lokalen Desktops und den zugehörigen Remote-Desktops im Rechenzentrum ausgeführt. Standardmäßig werden keine sicheren Tunnelverbindungen verwendet.
[Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]	Für die Kommunikation und Datenübertragungen zwischen Clientcomputern und dem Rechenzentrum wird die SSL-Verschlüsselung verwendet. Zu diesen Vorgängen zählen das Ein- und Auschecken von Desktops sowie das Replizieren von Daten von Clientcomputern in das Rechenzentrum, nicht jedoch die Übertragung von View Composer-Basis-Images. Sie umfassen Verbindungen zwischen Clientcomputern und View Transfer Server. Standardmäßig wird SSL nicht verwendet.
[Use SSL when provisioning desktops in Local Mode (SSL bei der Bereitstellung von Desktops im lokalen Modus verwenden)]	Bei Übertragungen der View Composer-Basis-Image-Dateien aus dem Transfer Server-Repository auf Clientcomputer wird die SSL-Verschlüsselung verwendet. Diese Vorgänge umfassen Verbindungen zwischen Clientcomputern und View Transfer Server. Standardmäßig wird SSL nicht verwendet.

Ändern der auf lokalen Desktops eingesetzten Verschlüsselungsmethode für das Generieren neuer Schlüssel

Standardmäßig verwendet View Connection Server AES-128 zur Verschlüsselung der virtuellen Festplattendatei (`.vmdk`), wenn Benutzer einen lokalen Desktop ein- und auschecken. Wenn Sie eine sicherere Verschlüsselung wünschen, können Sie die Verschlüsselungsmethode in AES-192 oder AES-256 ändern, indem Sie in View LDAP auf Ihrem View Connection Server-Host eine globale Eigenschaft bearbeiten.

Nach dem Ändern der Verschlüsselungsmethode für lokale Desktops wird die neue Methode beispielsweise zum Generieren eines neuen Schlüssels verwendet, wenn ein lokaler Desktop zum ersten Mal ausgecheckt wird. Zuvor generierte Schlüssel werden nicht geändert. Weitere Informationen zum Ändern der Verschlüsselungsmethode für vorhandene lokale Desktops finden Sie unter „Ändern der Verschlüsselungsmethode für einen vorhandenen lokalen Desktop“, auf Seite 316.

Verwenden Sie zur Änderung von View LDAP das Dienstprogramm ADSI-Editor. Das Dienstprogramm ADSI-Editor ist zusammen mit der View Connection Server-Instanz installiert. Wenn Sie View LDAP auf einer View Connection Server-Instanz ändern, werden diese Änderungen auf alle replizierten View Connection Server-Instanzen übertragen.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion.

Vorgehensweise

1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host.

2 Wählen Sie oder stellen Sie eine Verbindung mit **[DC=vdi, DC=vmware, DC=int]** her.

3 Setzen Sie für das Objekt **[CN=Common, OU=Global, OU=Properties]** das Attribut **[pae-mVDIOfflineUpdateFrequency]** auf den Wert der neuen Verschlüsselungsmethode.

Sie können den Wert für die Verschlüsselungsmethode auf **AES-128**, **AES-192** oder **AES-256** festlegen. Der Standardwert lautet **AES-128**.

Ändern der Verschlüsselungsmethode für einen vorhandenen lokalen Desktop

Bearbeiten Sie den Eintrag **[pae-VM]** für den lokalen Desktop in View LDAP auf Ihrem View Connection Server-Host, um die Verschlüsselungsmethode für einen vorhandenen lokalen Desktop zu ändern.

Verwenden Sie zur Änderung von View LDAP das Dienstprogramm ADSI-Editor. Das Dienstprogramm ADSI-Editor ist zusammen mit der View Connection Server-Instanz installiert. Wenn Sie View LDAP auf einer View Connection Server-Instanz ändern, werden diese Änderungen auf alle replizierten View Connection Server-Instanzen übertragen.

Voraussetzungen

- Ändern Sie die Verschlüsselungsmethode für lokale Desktops. Siehe „Ändern der auf lokalen Desktops eingesetzten Verschlüsselungsmethode für das Generieren neuer Schlüssel“, auf Seite 315.
- Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogramms ADSI-Editor mit Ihrer Windows-Betriebssystemversion.

Vorgehensweise

1 Checken Sie den lokalen Desktop wieder ein, wenn er ausgecheckt ist, und entfernen Sie alle vorhandenen lokalen Dateien.

2 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host.

3 Wählen Sie oder stellen Sie eine Verbindung mit **[DC=vdi, DC=vmware, DC=int]** her.

4 Löschen Sie im Eintrag **[pae-VM]** für den lokalen Desktop die Werte für die Attribute **[pae-mVDIOfflineAuthKey]**, **[pae-mVDIOfflineDataKey]** und **[pae-mVDIOfflineObfuscationKey]**.

5 Checken Sie den lokalen Desktop aus.

View Connection Server generiert neue Schlüssel für den lokalen Desktop. Die neuen Schlüssel weisen den Wert der neuen Verschlüsselungsmethode auf.

Ermitteln der Auswirkung von Deduplizierung und Komprimierung auf Datenübertragungen

Sie können ermitteln, in welchem Umfang Deduplizierung und Komprimierung die Menge an Daten verringert, die während eines Übertragungsvorgangs über das Netzwerk gesendet wird. Sie können die Größe von Datenübertragungen ermitteln, indem Sie die View Client with Local Mode-Protokolle auf dem Clientcomputer überprüfen.

Während eines Eincheckvorgangs oder einer Replikation zeigt der lokale Desktop an, welche Datenmenge an den Remote-Desktop im Rechenzentrum übertragen wird, wenn keine Optimierung stattfindet. Diese Menge gibt nicht die tatsächliche Datenmenge wieder, die über das Netzwerk gesendet wird. Es wird unabhängig davon, ob Sie Deduplizierung und Komprimierung aktiviert haben, immer die gleiche Zahl angezeigt.

Wenn Sie beide Funktionen aktivieren, entfernt View Client mittels Deduplizierung zunächst redundante Datenblöcke aus den Daten, die übertragen werden sollen. Als Nächstes komprimiert View Client entweder die verbleibenden Daten oder ermittelt, dass die Daten nicht komprimiert werden können.

Lesen der View Client with Local Mode-Protokolle

Zum Generieren von Protokolleinträgen, die Statistiken zu Deduplizierung und Komprimierung anzeigen, müssen Sie die Protokolle auf den Modus `Debug` festlegen.

Tabelle 14-5 zeigt den Speicherort der View Client with Local Mode-Protokolle auf dem Clientcomputer.

Tabelle 14-5. Speicherort der View Client with Local Mode-Protokolle

Betriebssystem	Pfad
Windows 7 und Windows Vista	C:\Benutzer*Benutzername*\AppData\VMware\VDM\Logs\
Windows XP	C:\Dokumente und Einstellungen*Benutzername*\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Logs\

Wenn ein lokaler Desktop eingecheckt oder repliziert wird, übertragt View Transfer Server die Daten, die seit dem letzten Auscheck- oder Replikationsvorgang auf dem lokalen Desktop generiert wurden. Sie können die potenzielle Größe einer Datenübertragung einschätzen, wenn Sie wissen, wie lange auf dem Desktop neue Daten generiert wurden. Der folgende Beispielprotokolleintrag zeigt die Dauer (in Minuten) seit dem letzten Auscheck- oder Replikationsvorgang an:

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: Total checkin size over 34 minutes:
```

Ermitteln der Auswirkung von Deduplizierung und Komprimierung

Die Protokolleinträge `GetTotalCheckinSize` zeigen die vorausgesagte Größe der Übertragung, bevor die Übertragung stattfindet. Diese Angaben umfassen alle Festplatten des lokalen Desktops, von denen Daten übertragen werden.

Der folgende Beispieleintrag zeigt die Datenmenge, die während eines Eincheckvorgangs nicht per Deduplizierung optimiert wird. Es handelt sich um die von View vorausgesagte Datenmenge für die Übertragung.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: non-dedupe: 2 MB
```

In den folgenden Beispieleinträgen zeigt der Eintrag `parent-dedupe` die Datenmenge, die per Deduplizierung in View Transfer Server optimiert wird. Der Eintrag `self-dedupe` zeigt den Umfang der Deduplizierung auf dem Clientcomputer. Addieren Sie die Zahlen in diesen Einträgen, um die Gesamtdatenmenge abzuleiten, die per Deduplizierung optimiert wird.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: parent-dedupe: 871 MB
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: self-dedupe: 0 MB
```

Die Protokolleinträge `Replication statistics` zeigen die tatsächlichen Datenmengen, die über das Netzwerk gesendet wurden. Es werden getrennte Statistiken für jede Festplatte eines lokalen Desktops generiert, von der Daten übertragen werden.

Im folgenden Beispiel zeigen die Einträge `parent-dedupe` und `self-dedupe` Statistiken zur Deduplizierung, respektive auf der View Transfer Server-Instanz und dem Clientcomputer.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Replication statistics:
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Parent dedup: 871.139 MB
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Self dedup: 0 MB
```

Der folgende Beispieleintrag zeigt die Datenmenge, die während einer Übertragung komprimiert wurde:

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Compression: 0.000 MB compressed to 0.000 MB
```

Der folgende Beispieleintrag zeigt die Datenmenge, die nicht komprimiert wurde.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm] Raw
data: 2.198 MB
```

In diesem Beispiel zeigt der lokale Desktop eine Meldung wie beispielsweise `"Transferring 871MB"`. Diese Datenmenge wurde jedoch mittels Deduplizierung verringert. Wenngleich die verbleibenden Daten nicht komprimiert werden konnten, wurden nur 2,198 MB Daten über das Netzwerk übertragen.

Optimierung des Gastdateisystems bei Datenübertragungen

Bei Übertragungsvorgängen verringert View Transfer Server die Anzahl an Daten, die über das Netzwerk gesendet werden müssen, indem die Vorteile der Gastdateisystem-Optimierung genutzt werden.

Wenn eine virtuelle Desktop-Maschine eine primäre NTFS-Partition enthält, überträgt View Transfer Server die von NTFS zugewiesenen Blöcke. Nicht zugewiesene Blöcke werden nicht übertragen. Auf diese Weise wird die Gesamtanzahl an zu übertragenden Blöcken verringert.

Die Optimierung des Gastdateisystems erfolgt nur, wenn Daten aus primären NTFS-Partitionen übertragen werden. View Transfer Server führt diese Optimierung weder für erweiterte Partitionen oder über die Verwaltung logischer Datenträger erstellte Partitionen noch für komprimierte NTFS-Volumes auf virtuellen Windows 7- oder Windows Vista-Maschinen durch.

Die Optimierung des Gastdateisystems unterscheidet sich von der Datendeduplizierung und -komprimierung, die zwar auch der Optimierung von Datenübertragungen dienen, aber vom Gastbetriebssystem des Desktops unabhängig sind. Weitere Informationen zu diesen Vorgängen finden Sie unter „Optimieren der Datenübertragung zwischen Hostcomputern lokaler Desktops und dem Rechenzentrum“, auf Seite 313.

Konfigurieren der Ressourcennutzung für Endpunkte

Für die Verwendung auf einem lokalen System ausgecheckte View-Desktops nutzen standardmäßig die Arbeitsspeicher- und CPU-Optionen dieses Hosts. Die virtuellen Netzwerkkarten des Desktops verwenden NAT, um die IP- und MAC-Adressen des Hosts gemeinsam zu verwenden. Dieses Standardverhalten kann geändert werden.

Außerkraftsetzen der lokalen Nutzung von Arbeitsspeicher- und CPU-Ressourcen

Nachdem ein lokaler Desktop ausgescheckt ist, nutzt er die Arbeitsspeicher- und CPU-Ressourcen des lokalen Systems unabhängig von den Arbeitsspeicher- und CPU-Einstellungen für die virtuelle Maschine in vCenter Server. Dieses Standardverhalten kann außer Kraft gesetzt werden.

Die RAM-Größe, die einem zur Verwendung im lokalen Modus ausgecheckten View-Desktop zugewiesen ist, wird standardmäßig automatisch an eine bestimmte Größe des RAM auf dem Clienthost angepasst.

In der Formel wird berücksichtigt, wie viel Arbeitsspeicher verfügbar ist, um diesen zwischen Host und lokalem View-Desktop aufzuteilen. Für ein Windows XP-Betriebssystem sind mindestens 512 MB Arbeitsspeicher erforderlich. Für ein Windows 7- oder Windows Vista-Betriebssystem mit 32-Bit ist mindestens 1 GB Arbeitsspeicher erforderlich. Die verfügbare Arbeitsspeichergröße, die aufgeteilt werden kann, ist der gesamte RAM auf dem Host abzüglich der Mindestanforderungen an den RAM für Host- und Gastbetriebssysteme.

Tabelle 14-7. Für lokale View-Desktops vorgesehener Arbeitsspeicher

Arbeitsspeicherzuweisung	Windows XP-Gastsysteme	Windows 7- und Windows Vista-Gastsysteme
Minimal	512MB	1 GB
Best Effort	512MB + (verfügbarer RAM/2)	1GB + (verfügbarer RAM/2)
Maximal	2GB	4GB

Wenn ein Windows 7-Host beispielsweise über insgesamt 2 GB Arbeitsspeicher verfügt, würde die lokale Ausführung eines View-Desktops mit Windows 7 2 GB Arbeitsspeicher erfordern, wobei 1 GB Arbeitsspeicher dem Host und 1 GB Arbeitsspeicher dem lokalen View-Desktop zugeweisen wird. Wenn der Host über 3 GB Arbeitsspeicher verfügen würde, würden 1,5 GB Arbeitsspeicher dem Host und 1,5 GB Arbeitsspeicher dem lokalen View-Desktop zugewiesen werden.

HINWEIS Bei der automatischen Anpassung der Arbeitsspeicherzuweisung wird für den Arbeitsspeicher des lokalen Desktops nie ein niedrigerer Wert als der in vCenter Server konfigurierte Wert festgelegt.

Gleichermaßen kann der lokale View-Desktop bis zu zwei CPUs nutzen, die auf dem Clienthost verfügbar sind, wenn auf dem View-Desktop Windows Vista oder ein höheres Betriebssystem ausgeführt wird.

Sie können die Standardwerte ändern und den Geltungsbereich der Einstellung festlegen. Die Einstellung kann auf alle lokalen Desktops auf dem Client oder, abhängig von der Einstellung, auf einen bestimmten Desktop bzw. auf alle Desktops einer bestimmten View Connection Server-Instanz angewendet werden, zu deren Verwendung ein spezifischer Benutzer auf dem Client berechtigt ist.

Zum Ändern dieser Standardwerte müssen Sie die Windows-Registrierungseinstellungen konfigurieren. Zur Bereitstellung dieser Registrierungseinstellungen können Sie standardmäßige Windows-Tools wie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden.

Voraussetzungen

- Wenn Sie eine bestimmte Anzahl an CPUs festlegen möchten, die der lokale Desktop verwenden kann, schalten Sie den lokalen Desktop aus.
- Da Sie den Geltungsbereich der Einstellung in vielen Fällen angeben können, bestimmen Sie die IDs, die Sie festlegen müssen.

Tabelle 14-6. In den Registrierungseinstellungen verwendete IDs für die Ressourcennutzung im lokalen Modus

Geltungsbereich	Bezeichnung der Variablen	Beschreibung
Broker-spezifisch	*Broker-GUID*	GUID (Globally Unique Identifier) für die View Connection Server-Instanz oder -Gruppe. Legen Sie die GUID über den Befehl `vdmadmin -C` fest. Siehe „Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C““, auf Seite 388.
Benutzerspezifisch	*Remote-Benutzer_SID*	Die Sicherheits-ID des Endbenutzers. Verwenden Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host und suchen Sie nach dem Wert des Felds **[pae-SIDString]** von **[CN=*Maschinen-CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** .
Desktop-spezifisch	*Desktop-ID*	Die ID des View-Desktops. Verwenden Sie das Dienstprogramm ADSI-Editor auf einem View Connection Server-Host. Die ID ist in **[OU=Applications]** von **[DC=vdi,DC=vmware,DC=int]** aufgeführt. Die Desktop-ID ist der Distinguished Name, der den Anzeigenamen des Desktop-Pools verwendet: **[CN=*Pool-Anzeigename*,OU=Applications,DC=vdi,DC=vmware,DC=int.]**

Die Broker-GUID können Sie auch in der Datei `mvdi.lst` auf Ihrem Clientcomputer finden. Unter Windows XP befindet sich die Datei im Ordner `C:\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Anwendungsdaten\VMware\VDM`. Öffnen Sie die Datei und suchen Sie nach `brokerGUID`. Die Sicherheits-ID des Remote-Benutzers ist ebenfalls in dieser Datei aufgelistet. Öffnen Sie die Datei und suchen Sie nach `user-sid`.

Vorgehensweise

- Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop lediglich die in vCenter Server konfigurierte Arbeitsspeichergröße verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup`
Broker- und benutzerspezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Remote-Benutzer-SID`*`\disableOfflineDesktopMemoryScaleup`

  Der Wert 1 gibt an, dass `disableOfflineDesktopMemoryScaleup` aktiviert ist, der Wert 0 weist darauf hin, dass die Einstellung deaktiviert ist.

- Um eine bestimmte Arbeitsspeichergröße für den View-Desktop festzulegen, wenn dieser lokal ausgeführt wird, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel zur Angabe eines Werts in MB (bis zu 32 GB) hinzuzufügen, und stellen Sie das GPO bereit.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Remote-Benutzer-SID`*`\offlineDesktopDefaultMemoryScaleupValue`
Desktop-spezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Remote-Benutzer-SID`*`\`*`Desktop-ID`*`\offlineDesktopDefaultMemoryScaleupValue`

  Bei Angabe eines zu hohen Werts kann der lokale Desktop nicht eingeschaltet werden und es wird eine Fehlermeldung angezeigt.

- Um einen Desktop auszuchecken, der so konfiguriert wurde, dass er mehr Arbeitsspeicher benötigt als auf dem Clienthost verfügbar ist, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um den folgenden Registrierungsschlüssel zur Angabe eines Werts für die zu berichtende Arbeitsspeichergröße des lokalen Clients in MB hinzuzufügen, und stellen Sie das GPO bereit.

  `HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Remote-Benutzer-SID`*`\offlineDesktopReportedHostMemoryValue`

  Die Einstellung dieses Wertes auf größer oder gleich dem vom View-Desktop geforderten Speicher ermöglicht es Ihnen, den View-Desktop auszuchecken und auszuführen, wenn auf dem Client genug Speicher vorhanden ist, um die virtuelle Maschine auszuführen.

  Wenn der Client nicht über ausreichend Speicher verfügt, können Sie die Einstellung `offlineDesktopDefaultMemoryScaleupValue` in Verbindung mit der Einstellung `offlineDesktopReportedHostMemoryValue` verwenden.

  Wenn Ihr Clientsystem z. B. 2 GB Speicher hat und der View-Desktop laut Konfiguration 2 GB Speicher erfordert, können Sie den View-Desktop nicht auschecken, da ein gewisser Anteil des Speichers für vom Client gehostete Virtualisierung notwendig ist. Sie können jedoch die Registrierungseinstellung `offlineDesktopReportedHostMemoryValue = 2048` verwenden, damit Sie den Desktop auschecken können, und die Registrierungseinstellung `offlineDesktopDefaultMemoryScaleupValue = 1024` verwenden, damit der View-Desktop nur 1 GB Speicher verwendet, wenn er lokal ausgeführt wird.

- Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop lediglich die in vCenter Server konfigurierte Anzahl an CPUs verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOffline-DesktopCPUScaleup`
Broker- und benutzerspezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broke-GUID`*`\`*`Re-mote-Benutzer-SID`*`\disableOfflineDesktopCPUScaleup`

  Der Wert 1 gibt an, dass `disableOfflineDesktopCPUScaleup` aktiviert ist, der Wert 0 weist darauf hin, dass die Einstellung deaktiviert ist.

- Um eine bestimmte Anzahl an CPUs für den View-Desktop festzulegen, wenn dieser lokal ausgeführt wird, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel zur Angabe der Anzahl an CPUs (bis zu 2) hinzuzufügen, und stellen Sie das GPO bereit.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Re-mote-Benutzer-SID`*`\offlineDesktopDefaultCPUScaleupValue`
Desktop-spezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker-GUID`*`\`*`Re-mote-Benutzer-SID`*`\`*`Desktop-ID`*`\offlineDesktopDefaultCPUSca-leupValue`

  Bei Angabe eines ungültigen Werts wird dieser ignoriert und der Standardwert verwendet. Wenn Sie mehr CPUs festlegen, als auf dem Host verfügbar sind, wird der lokale Desktop nicht gestartet und es wird eine Fehlermeldung angezeigt. Wenn Sie einen höheren Wert als 2 festlegen, wird der Wert 2 verwendet.

Mit Ausnahme der Einstellung, über welche die erforderliche Arbeitsspeichergröße geringer sein darf als der festgelegte Wert in vCenter Server, werden die Einstellungen übernommen, wenn der lokale Desktop gestartet wird. Diese Einstellung ist bei einem ausgecheckten Desktop schreibgeschützt.

Ändern des Netzwerktyps von NAT in Bridged

Der virtuelle Netzwerktyp eines View-Desktops wird standardmäßig in NAT (Network Address Translation) geändert, wenn der Desktop zur Verwendung auf einem lokalen System ausgecheckt wird. Sie können dieses Verhalten außer Kraft setzen und ein Bridged-Netzwerk verwenden, sodass der View-Desktop über eine eigene Netzwerkidentität verfügt.

Bei einem Bridged-Netzwerk wird der virtuelle Netzwerkadapter im View-Desktop mit dem physischen Netzwerkadapter im Hostcomputer verbunden. In einem Bridged-Netzwerk ist der View-Desktop für andere Computer im Netzwerk sichtbar und der Desktop muss über eine eigene IP-Adresse verfügen.

Bei NAT wird eine virtuelle Maschine für die gemeinsame Verwendung der IP- und MAC-Adressen des Hosts konfiguriert. Der View-Desktop und der Clienthost verwenden eine einzige Netzwerkidentität innerhalb des Netzwerks.

Um diese Standardeinstellungen für alle lokalen Desktops oder für bestimmte lokale Desktop auf einem Clienthost zu ändern, müssen Windows-Registrierungseinstellungen konfiguriert werden. Zur Bereitstellung dieser Registrierungseinstellungen können Sie standardmäßige Windows-Tools wie Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) verwenden.

Voraussetzungen

- Da Sie den Geltungsbereich der Einstellung in vielen Fällen angeben können, bestimmen Sie die IDs, die Sie festlegen müssen.

  Tabelle 14-8. In den Registrierungseinstellungen verwendete IDs für die Ressourcennutzung im lokalen Modus

Geltungsbereich	Bezeichnung der Variablen	Beschreibung
Broker-spezifisch	*Broker-GUID*	GUID (Globally Unique Identifier) für die View Connection Server-Instanz oder -Gruppe. Legen Sie die GUID über den Befehl `vdmadmin –C` fest. Siehe „Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C"", auf Seite 388.
Benutzerspezifisch	*Remote-Benutzer_SID*	Die Sicherheits-ID des Endbenutzers. Verwenden Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host und suchen Sie nach dem Wert des Felds **[pae-SIDString]** von **[CN=*Maschinen-CN*,OU=Servers,DC=vdi,DC=vmware,DC=int]** .
Desktop-spezifisch	*Desktop-ID*	Die ID des View-Desktops. Verwenden Sie das Dienstprogramm ADSI-Editor auf einem View Connection Server-Host. Die ID ist in **[OU=Applications]** von **[DC=vdi,DC=vmware,DC=int]** aufgeführt. Die Desktop-ID ist der Distinguished Name, der den Anzeigenamen des Desktop-Pools verwendet: **[CN=*Pool-Anzeigename*,OU=Applications,DC=vdi,DC=vmware,DC=int.]**

  Die Broker-GUID können Sie auch in der Datei `mvdi.lst` auf Ihrem Clientcomputer finden. Unter Windows XP befindet sich die Datei im Ordner `C:\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Anwendungsdaten\VMware\VDM`. Öffnen Sie die Datei und suchen Sie nach `brokerGUID`. Die Sicherheits-ID des Remote-Benutzers ist ebenfalls in dieser Datei aufgelistet. Öffnen Sie die Datei und suchen Sie nach `user–sid`.

Vorgehensweise

- Um das Standardverhalten außer Kraft zu setzen, sodass der lokale Desktop ein Bridged-Netzwerk verwendet, führen Sie die folgenden Schritte aus: Erstellen Sie ein GPO, um einen der folgenden Registrierungsschlüssel hinzuzufügen, und stellen Sie das GPO bereit. Setzen Sie den Schlüssel auf 1.

Geltungsbereich der Einstellung	Pfad
Gesamter Client	`HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking`
Connection Server- und benutzerspezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker–GUID`*`\`*`Remote–Benutzer–SID`*`\offlineDesktopUseBridgedNetworking`
Desktop-spezifisch	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`Broker–GUID`*`\`*`Remote–Benutzer–SID`*`\`*`Desktop–ID`*`\offlineDesktopUseBridgedNetworking`

  Durch den Wert 1 wird festgelegt, dass der Desktop den Bridged-Netzwerktyp verwendet. Der Wert 0 legt die Verwendung von NAT fest (Standardeinstellung).

Diese Einstellung wird angewendet, wenn der Endbenutzer den lokalen Desktop einschaltet.

Konfigurieren eines HTTP-Caches für die Bereitstellung lokaler Desktops über ein WAN

Sie können einen HTTP-Cache verwenden, um die Bereitstellung lokaler Linked-Clone-Desktops zu vereinfachen. Die Konfiguration eines HTTP-Caches bietet Vorteile für Remote-Niederlassungen und Zweigstellen die über ein WAN mit dem Rechenzentrum verbunden sind. Der HTTP-Cache verringert die Leistungskosten für die Übertragung von View Composer-Basis-Images über ein WAN.

Wenn Sie Linked-Clone-Desktops für die Verwendung im lokalen Modus in Remote-Niederlassungen konfigurieren, verfügt Ihr WAN möglicherweise nicht über eine ausreichende Bandbreite für einen schnellen Download von View Composer-Basis-Images direkt auf jeden lokalen Computer. Beispielsweise kann die wiederholte Übertragung eines Basis-Images mit einer Größe von 6 GB problematisch sein.

Wenn Sie einen HTTP-Cache eingerichtet haben, wird das Basis-Image im Cache des Proxy-Servers gespeichert, sobald der erste Benutzer einen Desktop auscheckt. Werden dann Desktops von nachfolgenden Benutzern ausgecheckt, wird das Basis-Image innerhalb der lokalen Niederlassung über das LAN übertragen.

Zum Beenden eines Vorgangs zum Auschecken muss View Transfer Server weiterhin jede Linked-Clone-Betriebssystemfestplatte und jede persistente Festplatte eines Benutzers aus dem Rechenzentrum über das WAN übertragen. Dabei beträgt die Größe dieser Festplatten jedoch nur einen Bruchteil der Basis-Image-Größe.

1 Konfigurieren von View Connection Server für die Unterstützung der HTTP-Zwischenspeicherung von View Composer-Basis-Images auf Seite 323

   Um über einen zur Zwischenspeicherung eingesetzten Proxy-Server View Composer-Basis-Images und andere Daten zwischen lokalen Desktops und dem Rechenzentrum übertragen zu können, müssen bestimmte Einstellungen in View Connection Server konfiguriert werden.

2 Beschränken der Größe von Basis-Image-Paketdateien für die Zwischenspeicherung auf Seite 324

   Ein View Composer-Basis-Image-Paket kann Dateien mit einer Größe von mehr als einem Gigabyte enthalten. Diese Größe wird für die Zwischenspeicherung auf vielen Proxy-Servern nicht unterstützt. Sie können View Transfer Server so konfigurieren, dass Basis-Image-Pakete in Dateien unterteilt werden, deren Größe die Kapazität des Proxy-Servercaches nicht übersteigt.

3 Konfigurieren von Clientcomputern für die Datenübertragung über einen Proxy-Server auf Seite 325

   Zur Unterstützung der HTTP-Zwischenspeicherung müssen Sie die Clientcomputer, die lokale Desktops hosten, für die Übertragung der Desktop-Daten über einen zur Zwischenspeicherung eingesetzten Proxy-Server konfigurieren. Sie müssen die Clientcomputer zudem so konfigurieren, dass sie für Internetverbindungen die HTTP-Adresse des Proxy-Servers verwenden.

4 Konfigurieren eines Proxy-Servers für das Zwischenspeichern von View Composer-Basis-Images auf Seite 326

   Wenn Sie einen Proxy-Server für die Unterstützung der HTTP-Zwischenspeicherung für lokale Desktops einrichten, müssen Sie die Größe des Caches und die HTTP-Verbindungsmethode konfigurieren.

Konfigurieren von View Connection Server für die Unterstützung der HTTP-Zwischenspeicherung von View Composer-Basis-Images

Um über einen zur Zwischenspeicherung eingesetzten Proxy-Server View Composer-Basis-Images und andere Daten zwischen lokalen Desktops und dem Rechenzentrum übertragen zu können, müssen bestimmte Einstellungen in View Connection Server konfiguriert werden.

Zur Konfiguration der SSL-Verschlüsselung müssen für die folgenden zwei Datentypen zwei separate View-Einstellungen verwendet werden:

- View Composer-Basis-Images

- Andere Linked-Clone-Desktop-Daten, einschließlich Betriebssystemfestplatten und persistente Festplatten

Die SSL-Verschlüsselung muss für die Übertragung von Basis-Image-Paketdateien vom Transfer Server-Repository an lokale Computer deaktiviert werden. Durch die Deaktivierung von SSL kann der Proxy-Server auf die Inhalte der Paketdateien zugreifen und diese zwischenspeichern. Die Basis-Image-Daten werden durch die Deaktivierung von SSL nicht offengelegt. Die Daten werden bei der Veröffentlichung des Basis-Images im Transfer Server-Repository verschlüsselt und diese Verschlüsselung bleibt erhalten, wenn die Daten über das WAN auf den Proxy-Server heruntergeladen werden.

Sie können wählen, ob die SSL-Verschlüsselung auch für die Übertragung aller anderen Daten eines lokalen Desktops verwendet werden soll. Um die Übertragung anderer Daten lokaler Desktops über einen zur Zwischenspeicherung eingesetzten Proxy-Server zuzulassen, müssen Sie den Proxy-Server so konfigurieren, dass die Verwendung der HTTP-CONNECT-Methode zulässig ist. Alternativ aktivieren Sie die SSL-Verschlüsselung für Vorgänge im lokalen Modus für View Connection Server.

Bei Verwendung der SSL-Verschlüsselung müssen Sie die Einstellungen des Proxy-Servers nicht ändern. Die SSL-Verschlüsselung kann jedoch zu Leistungsbeeinträchtigungen bei der Übertragung von Linked-Clone-Betriebssystemfestplatten und persistenten Linked-Clone-Festplatten führen.

Diese SSL-Einstellungen müssen auf jeder View Connection Server-Instanz konfiguriert werden, die View-Dienste für Clients bereitstellt, für die Sie die HTTP-Zwischenspeicherung konfigurieren.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie im Fenster mit den View-Servern eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Deaktivieren Sie die Einstellung **[Use SSL when provisioning desktops in local mode (SSL bei der Bereitstellung von Desktops im lokalen Modus verwenden)]** .

   Mit dieser Einstellung wird SSL für das Herunterladen von Basis-Image-Paketdateien aus dem Transfer Server-Repository auf lokale Computer deaktiviert.

4 Wenn Sie für den zur Zwischenspeicherung eingesetzten Proxy-Server nicht die Verwendung der HTTP-CONNECT-Methode festlegen, wählen Sie die Einstellung **[Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]** .

   Diese Einstellung wirkt sich auf die Übertragung aller weiteren Daten lokaler Desktops aus.

Beschränken der Größe von Basis-Image-Paketdateien für die Zwischenspeicherung

Ein View Composer-Basis-Image-Paket kann Dateien mit einer Größe von mehr als einem Gigabyte enthalten. Diese Größe wird für die Zwischenspeicherung auf vielen Proxy-Servern nicht unterstützt. Sie können View Transfer Server so konfigurieren, dass Basis-Image-Pakete in Dateien unterteilt werden, deren Größe die Kapazität des Proxy-Servercaches nicht übersteigt.

Wenn Sie ein Paket im Transfer Server-Repository veröffentlichen, erstellt View Transfer Server Paketdateien mit der angegebenen Größe. Die maximale Größe muss vor dem Veröffentlichen von Paketen im Repository konfiguriert werden. View Transfer Server unterteilt keine vorhandenen Paketdateien, um die maximale Größe einzuhalten.

Dieser Wert kann auf jeder View Connection Server-Instanz in einer replizierten Gruppe festgelegt werden. Wenn Sie View LDAP ändern, werden diese Änderungen auf alle replizierten View Connection Server-Instanzen übertragen.

Voraussetzungen

Machen Sie sich mit der Verwendung des Befehls `vdmadmin` mit der Option –T vertraut. Siehe „Festlegen einer maximalen Größe für Paketdateien mithilfe der Option „-T“, um View Transfer Server-Pakete bei der Veröffentlichung zu unterteilen“, auf Seite 407.

Vorgehensweise

1 Öffnen Sie auf Ihrem View Connection Server-Computer eine Windows-Eingabeaufforderung.

2 Geben Sie den Befehl `vdmadmin` mit der Option –T ein.

```
vdmadmin –T [–packagelimit Größe_in_Byte]
```

Der Pfad zur ausführbaren Datei des Befehls `vdmadmin` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`.

Beispiel: Festlegen einer maximalen Größe für Paketdateien

Legen Sie für Paketdateien eine maximale Größe von 100MB fest, ab der die Dateien unterteilt werden.

```
vdmadmin –T –packagelimit 104857600
```

Zeigen Sie die aktuelle maximale Größe von Paketdateien an, ab der die Dateien unterteilt werden.

```
vdmadmin –T
```

Konfigurieren von Clientcomputern für die Datenübertragung über einen Proxy-Server

Zur Unterstützung der HTTP-Zwischenspeicherung müssen Sie die Clientcomputer, die lokale Desktops hosten, für die Übertragung der Desktop-Daten über einen zur Zwischenspeicherung eingesetzten Proxy-Server konfigurieren. Sie müssen die Clientcomputer zudem so konfigurieren, dass sie für Internetverbindungen die HTTP-Adresse des Proxy-Servers verwenden.

Um die Übertragung über einen Proxy-Server zu ermöglichen, fügen Sie einen Registrierungsschlüssel für die Clientcomputer hinzu. Sie können in Active Directory eine Gruppenrichtlinie für die Verwendung dieses Registrierungsschlüssels auf mehreren Computern in einer Domäne erstellen.

Vorgehensweise

1 Öffnen Sie den Windows-Registrierungs-Editor auf dem Clientsystem im lokalen Modus.

2 Erweitern Sie im linken Fensterbereich den Registrierungspfad.

Prozessor	Beschreibung
64 Bit	`HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM`
32 Bit	`HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM`

3 Klicken Sie auf **[Edit (Bearbeiten)] > [New (Neu)] > [String Value (Zeichenfolgenwert)]** und geben Sie **`useProxyForTransfer`** als neuen Wert ein.

4 Klicken Sie mit der rechten Maustaste auf den Eintrag **[useProxyForTransfer]** und anschließend auf **[Modify (Ändern)]** , geben Sie **`true`** ein und klicken Sie auf **[OK]** .

Der Eintrag wird zur Registrierung hinzugefügt.

5 Beenden Sie den Windows-Registrierungs-Editor.

6 Konfigurieren Sie auf dem Clientcomputer die Verbindungseinstellungen für den Internet Explorer so, dass der zur Zwischenspeicherung eingesetzte Proxy-Server verwendet wird.

   a Starten Sie Internet Explorer und klicken Sie auf **[Tools (Extras)] > [Internet Options (Internetoptionen)]** .

   b Wählen Sie auf der Registerkarte **[Connections (Verbindungen)]** die Option **[LAN Settings (LAN-Einstellungen)]** .

   c Klicken Sie auf **[Use a proxy server for your LAN (Proxy-Server für LAN verwenden)]** und anschließend auf **[Advanced (Erweitert)]** .

   d Geben Sie die Proxy-Adressen und Portnummern für die HTTP-, SSL-, FTP- und SOCKS-Verbindungen ein und klicken Sie auf **[OK]** .

Konfigurieren eines Proxy-Servers für das Zwischenspeichern von View Composer-Basis-Images

Wenn Sie einen Proxy-Server für die Unterstützung der HTTP-Zwischenspeicherung für lokale Desktops einrichten, müssen Sie die Größe des Caches und die HTTP-Verbindungsmethode konfigurieren.

Voraussetzungen

- Überprüfen Sie die mit dem Befehl `vdmadmin -T` festgelegte maximale Größe von Basis-Image-Paketdateien. Siehe „Beschränken der Größe von Basis-Image-Paketdateien für die Zwischenspeicherung“, auf Seite 324.
- Bestimmen Sie, ob Sie für Vorgänge im lokalen Modus SSL verwenden. Siehe „Konfigurieren von View Connection Server für die Unterstützung der HTTP-Zwischenspeicherung von View Composer-Basis-Images“, auf Seite 323.

Vorgehensweise

1 Konfigurieren Sie die maximale Größe des Caches auf dem Proxy-Server.

   Berücksichtigen Sie bei der Berechnung der maximalen Größe die Anzahl und die Größe der View Composer-Basis-Images, die von lokalen Desktops verwendet werden. Die Basis-Images werden als Paketdateien auf den Proxy-Server heruntergeladen. Berücksichtigen Sie auch andere Dateien, die auf dem Proxy-Server zwischengespeichert werden sollen.

2 Konfigurieren Sie die maximale Größe einzelner Dateien, die zwischengespeichert werden können.

   Die maximale Größe einzelner Dateien auf dem Proxy-Server muss mindestens der mit dem Befehl `vdmadmin -T` festgelegten maximalen Größe von Paketdateien entsprechen.

3 Wenn Sie die Einstellung **[Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]** für View Connection Server nicht aktivieren, legen Sie über die Zugriffssteuerungsliste auf dem Proxy-Server fest, dass Port 80 geöffnet wird und die CONNECT-Methode eine Verbindung über Port 80 herstellen kann.

   View Transfer Server verwendet die CONNECT-Methode zur Bereitstellung einer Tunnelverbindung über den Proxy-Server. View Transfer Server verwendet diese Verbindung zur Übertragung von Dateien und Daten, bei denen es sich nicht um View Composer-Basis-Images handelt, zwischen lokalen Desktops und dem Rechenzentrum. Bei Verwendung von Port 80 wird eine bessere Übertragungsleistung erzielt.

Konfigurieren des Taktsignalintervalls für Clientcomputer mit lokalem Desktop

Zum Ermitteln des Status ausgecheckter Desktops senden Clientcomputer mit lokalen Desktops in regelmäßigen Intervallen Taktsignalinformationen an View Connection Server. Das standardmäßige Taktsignalintervall beträgt für alle Clientcomputer fünf Minuten. Sie können das Taktsignalintervall für alle Clientcomputer ändern. Zudem können Sie ein individuelles Taktsignalintervall für einen bestimmten Clientcomputer festlegen.

- Ändern des Taktsignalintervalls für alle Clientcomputer mit lokalem Desktop auf Seite 327

  Verwenden Sie das Dienstprogramm ADSI-Editor, um View LDAP auf Ihrem View Connection Server-Host zu bearbeiten und so das Taktsignalintervall für alle Clientcomputer mit lokalem Desktop zu ändern. Das Dienstprogramm ADSI-Editor ist zusammen mit der View Connection Server-Instanz installiert.

- Festlegen des Taktsignalintervalls für einen spezifischen Clientcomputer mit lokalem Desktop auf Seite 328

  Verwenden Sie den Windows-Registrierungs-Editor, um die Systemregistrierung auf dem Computer zu bearbeiten und so das Taktsignalintervall für diesen spezifischen Clientcomputer mit lokalem Desktop festzulegen.

Ändern des Taktsignalintervalls für alle Clientcomputer mit lokalem Desktop

Verwenden Sie das Dienstprogramm ADSI-Editor, um View LDAP auf Ihrem View Connection Server-Host zu bearbeiten und so das Taktsignalintervall für alle Clientcomputer mit lokalem Desktop zu ändern. Das Dienstprogramm ADSI-Editor ist zusammen mit der View Connection Server-Instanz installiert.

Wenn Sie View LDAP auf einer View Connection Server-Instanz ändern, werden diese Änderungen auf alle replizierten View Connection Server-Instanzen übertragen.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Dienstprogrammes ADSI-Editor mit Ihrer Windows Server-Betriebssystemversion.

Vorgehensweise

1 Starten Sie das Dienstprogramm ADSI-Editor auf Ihrem View Connection Server-Host.

2 Wählen Sie oder stellen Sie eine Verbindung mit **[DC=vdi, DC=vmware, DC=int]** her.

3 Setzen Sie für das Objekt **[CN=Common, OU=Global, OU=Properties]** das Attribut **[pae-mVDIOfflineUpdateFrequency]** auf ein neues Taktsignalintervall in Minuten.

   Sie müssen eine positive Ganzzahl eingeben. Dieses Attribut ist standardmäßig nicht festgelegt. Wenn es nicht festgelegt ist, beträgt der Standardwert fünf Minuten.

Das neue Taktsignalintervall wird übernommen, sobald ein Clientcomputer mit lokalem Desktop die nächste Taktsignalmeldung an View Connection Server sendet. Der View Connection Server-Dienst oder der Clientcomputer müssen nicht neu gestartet werden.

Wird auf einem Clientcomputer ein kleinerer Wert für das Taktsignalintervall eingegeben, verwendet View den Wert des Clientcomputers und nicht den der View Connection Server-Instanz. Standardmäßig ist das Taktsignalintervall auf Clientcomputern nicht festgelegt.

Festlegen des Taktsignalintervalls für einen spezifischen Clientcomputer mit lokalem Desktop

Verwenden Sie den Windows-Registrierungs-Editor, um die Systemregistrierung auf dem Computer zu bearbeiten und so das Taktsignalintervall für diesen spezifischen Clientcomputer mit lokalem Desktop festzulegen.

View verwendet das auf dem Clientcomputer festgelegte Taktsignalintervall nicht, wenn der Wert größer als der für das auf dem View Connection Server-Host festgelegte Taktsignalintervall ist. View verwendet immer den kleineren der beiden Werte. Das standardmäßige Taktsignalintervall für die View Connection Server-Instanz beträgt fünf Minuten.

Voraussetzungen

Auf der Microsoft TechNet-Website finden Sie Informationen zur Verwendung des Windows-Registrierungs-Editors in der Windows-Betriebssystemversion auf dem im lokalen Modus ausgeführten Clientsystem.

Vorgehensweise

1 Starten Sie den Windows-Registrierungs-Editor auf dem lokalen Desktop des Clientcomputers.

2 Fügen Sie einen neuen Registrierungsschlüssel mit der Bezeichnung **[policyUpdateFrequency]** hinzu.

Der Speicherort der Systemregistrierung hängt vom Prozessortyp des Clientcomputers ab.

Option	Aktion
64 Bit	Fügen Sie **[policyUpdateFrequency]** zu `HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM` hinzu.
32 Bit	Fügen Sie **[policyUpdateFrequency]** zu `HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM` hinzu.

3 Geben Sie für den Schlüsselwert **[policyUpdateFrequency]** das neue Taktsignalintervall in Millisekunden an.

Sie müssen eine positive Ganzzahl eingeben.

Manuelles Herunterladen eines lokalen Desktops an einem Standort mit unzureichenden Netzwerkverbindungen

Für Benutzer in einem Netzwerk mit sehr niedriger Bandbreite kann sich das Auschecken eines Desktops als problematisch erweisen, da mehrere Gigabyte an Daten heruntergeladen werden müssen. Um diese Benutzer zu unterstützen, können Sie die Desktop-Dateien manuell herunterladen und auf die Clientcomputer kopieren.

Angenommen, ein Benutzer arbeitet von zu Hause aus in einer ländlichen Umgebung mit einer DFÜ-Netzwerkverbindung. Der Benutzer arbeitet möglicherweise nie in der Hauptniederlassung, wo der Desktop auf den Laptop des Benutzers über das LAN ausgecheckt werden könnte.

In diesem Fall können Sie die Desktop-Dateien auf einen mobilen Datenträger, wie ein USB-Gerät oder eine DVD, manuell herunterladen. Nachdem der Benutzer den Datenträger von Ihnen erhalten hat, kann dieser die Dateien in ein bestimmtes Verzeichnis auf dem Clientcomputer kopieren und den Desktop aus dem View-Rechenzentrum auschecken.

Sie können diesen Ansatz nur für Linked-Clone-Desktops aus View Composer verwenden.

- Sie laden die View Composer-Basis-Image-Dateien manuell herunter.
- Wenn der Benutzer den Desktop auscheckt, müssen die Dateien der Linked-Clone-Betriebssystemfestplatte und der persistenten Festplatte noch über das Netzwerk heruntergeladen werden.

Die Dateien mit dem größten Umfang sind jedoch im Basis-Image enthalten. Ein Windows 7-Basis-Image kann zum Beispiel zwischen 6 und 10 GB umfassen. Die Betriebssystemfestplatte und die persistente Festplatte weisen nur einen Bruchteil dieser Größe auf.

1 Kopieren des Basis-Images aus dem Transfer Server-Repository auf Seite 329

   Wenn Sie einen Desktop zur Verwendung im lokalen Modus manuell auf einen Clientcomputer herunterladen möchten, müssen Sie das View Composer-Basis-Image auf ein tragbares Gerät kopieren. Das Basis-Image wird als Paket im Transfer Server-Repository veröffentlicht.

2 Kopieren der Basis-Image-Dateien auf den Clientcomputer auf Seite 330

   Wenn Sie einen Desktop zur Verwendung im lokalen Modus manuell auf einen Clientcomputer herunterladen möchten, müssen Sie die Basis-Image-Paketdateien von einem tragbaren Gerät auf den Clientcomputer kopieren.

3 Festlegen von Berechtigungen für die Verwendung kopierter Paketdateien durch View auf Seite 330

   Damit Vorgänge zum Auschecken für den lokalen Modus fortgesetzt werden können, müssen Berechtigungen für die Basis-Image-Paketdateien festgelegt werden, die in das Verzeichnis zum Auschecken auf dem Clientcomputer kopiert wurden.

4 Auschecken eines Desktops nach dem manuellen Kopieren des Basis-Images auf Seite 331

   Nachdem Sie das Basis-Image manuell auf den Clientcomputer kopiert haben und die Berechtigungen für die Paketdateien festgelegt haben, müssen Sie dem Benutzer den Vorgang zum Auschecken erläutern.

Kopieren des Basis-Images aus dem Transfer Server-Repository

Wenn Sie einen Desktop zur Verwendung im lokalen Modus manuell auf einen Clientcomputer herunterladen möchten, müssen Sie das View Composer-Basis-Image auf ein tragbares Gerät kopieren. Das Basis-Image wird als Paket im Transfer Server-Repository veröffentlicht.

Voraussetzungen

- Stellen Sie sicher, dass Sie View Manager zur Bereitstellung lokaler Desktops konfiguriert haben. Siehe „Übersicht über die Einrichtung einer Bereitstellung lokaler Desktops“, auf Seite 292.
- Stellen Sie sicher, dass Sie einen Linked-Clone-Desktop-Pool erstellt und ein Paket im Transfer Server-Repository veröffentlicht haben. Siehe „Veröffentlichen von Paketdateien im Transfer Server-Repository“, auf Seite 305.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

2 Wählen Sie im Bereich **[Contents (Inhalte)]** das Paket aus, das mit dem Desktop-Pool verknüpft ist, aus dem Sie einen Desktop auschecken möchten. Anschließend klicken Sie auf **[Details]** .

3 Stellen Sie sicher, dass der Desktop-Pool mit diesem Paket verknüpft ist.

4 Suchen Sie den Repository-Pfad, der die Paket-ID enthält.

   Beispiel: `\\MeinComputer.com\ImageRepository\Published\f222434a-e52a-4ce3-92d1-c14122fca996`

5 Kopieren Sie die Paketinhalte aus dem Transfer Server-Repository auf das tragbare Gerät.

   Sie müssen das gesamte Paketverzeichnis auf das tragbare Gerät kopieren.

Kopieren der Basis-Image-Dateien auf den Clientcomputer

Wenn Sie einen Desktop zur Verwendung im lokalen Modus manuell auf einen Clientcomputer herunterladen möchten, müssen Sie die Basis-Image-Paketdateien von einem tragbaren Gerät auf den Clientcomputer kopieren.

Voraussetzungen

- Stellen Sie sicher, dass der Benutzer View Client with Local Mode auf dem Clientcomputer installiert hat.
- Stellen Sie sicher, dass Sie die Paketdateien auf ein tragbares Gerät kopiert haben. Siehe „Kopieren des Basis-Images aus dem Transfer Server-Repository“, auf Seite 329.

Vorgehensweise

1 Stellen Sie das tragbare Gerät bereit, auf dem die Paketdateien des Desktop-Pools für den Benutzer gespeichert sind.

2 Kopieren Sie die Paketdateien in eine festgelegtes Verzeichnis zum Auschecken auf dem Clientcomputer.

Kopieren Sie die Dateien in ein Unterverzeichnis im Verzeichnis zum Auschecken, wobei das Unterverzeichnis den Anzeigenamen des Desktop-Pools trägt. Beispiel: Wenn Sie Dateien aus einem Desktop-Pool mit dem Anzeigenamen `LocalPool` herunterladen, kopieren Sie die Dateien unter *`Verzeichnis_zum_Auschecken`*`\LocalPool`.

Verzeichnis zum Auschecken	Beschreibung
Standardverzeichnis unter Windows 7 und Windows Vista	`C:\Benutzer\`*`Benutzername`*`\AppData\Local\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*
Standardverzeichnis unter Windows XP	`C:\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*
Benutzerdefiniertes Verzeichnis	Sie können ein eigenes Verzeichnis angeben. Beispiel: Um Dateien aus einem Desktop-Pool mit dem Anzeigenamen `LocalPool` herunterzuladen, können Sie diesen Pfad erstellen: `C:\CheckOutDirectory\LocalPool`.

Festlegen von Berechtigungen für die Verwendung kopierter Paketdateien durch View

Damit Vorgänge zum Auschecken für den lokalen Modus fortgesetzt werden können, müssen Berechtigungen für die Basis-Image-Paketdateien festgelegt werden, die in das Verzeichnis zum Auschecken auf dem Clientcomputer kopiert wurden.

Sie müssen den Schreibschutz für die Paketdateien entfernen und dem Benutzer die Berechtigung **Full control (Vollzugriff)** für das Verzeichnis und alle enthaltenen Dateien erteilen.

In diesem Beispiel wird gezeigt, wie Sie Berechtigungen auf einem Windows 7-Computer festlegen. Für andere Betriebssysteme weichen die erforderlichen Schritte möglicherweise etwas ab.

Voraussetzungen

Stellen Sie sicher, dass Sie die Paketdateien in ein Verzeichnis auf dem Clientcomputer kopiert haben. Siehe „Kopieren der Basis-Image-Dateien auf den Clientcomputer“, auf Seite 330.

Vorgehensweise

1 Melden Sie sich am Windows 7-Gastbetriebssystem an, klicken Sie auf das Symbol **[Libraries (Bibliotheken)]** und navigieren Sie zum Verzeichnis zum Auschecken.

2 Klicken Sie mit der rechten Maustaste auf das Verzeichnis zum Auschecken und anschließend auf **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Security (Sicherheit)]** auf **[Edit (Bearbeiten)]** .

4 Wählen Sie in der Liste der Gruppen- oder Benutzernamen den Namen des Benutzers, der den Desktop auschecken möchte.

   Wenn der Benutzername nicht in der Liste enthalten ist, klicken Sie auf **[Add (Hinzufügen)]** und fügen Sie den Benutzernamen hinzu.

5 Aktivieren Sie die Option **[Full control (Vollzugriff)]** in der Spalte **[Allow (Zulassen)]** und klicken Sie auf **[OK]** .

6 Deaktivieren Sie auf der Registerkarte **[General (Allgemein)]** die Option **[Read-only (Only applies to files in folder) (Nur Lesen (Gilt nur für Dateien im Ordner))]** .

   Stellen Sie sicher, dass das Kontrollkästchen deaktiviert ist.

7 Stellen Sie im Dialogfeld **[Confirm Attribute Changes (Änderungen der Attribute bestätigen)]** sicher, dass die Option **[Apply changes to this folder, subfolders and files (Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen)]** ausgewählt ist, und klicken Sie auf **[OK]** .

Auschecken eines Desktops nach dem manuellen Kopieren des Basis-Images

Nachdem Sie das Basis-Image manuell auf den Clientcomputer kopiert haben und die Berechtigungen für die Paketdateien festgelegt haben, müssen Sie dem Benutzer den Vorgang zum Auschecken erläutern.

Voraussetzungen

- Stellen Sie sicher, dass View Client with Local Mode auf dem Clientcomputer installiert ist.
- Stellen Sie sicher, dass Berechtigungen für die Verwendung der Paketdateien festgelegt wurden, die auf den Clientcomputer kopiert wurden. Siehe „Festlegen von Berechtigungen für die Verwendung kopierter Paketdateien durch View“, auf Seite 330.

Vorgehensweise

1 Starten Sie VMware View Client auf dem Clientcomputer, stellen Sie eine Verbindung zu View Connection Server her, melden Sie sich an der View Connection Server-Instanz an und wählen Sie einen Desktop-Pool.

2 Klicken Sie auf den nach unten weisenden Pfeil neben dem Desktop-Pool und klicken Sie auf **[Check out (Auschecken)]** .

3 (Optional) Wenn Sie die Paketdateien in ein benutzerdefiniertes Verzeichnis kopiert haben, konfigurieren Sie View Client für das Auschecken des Desktops in das benutzerdefinierte Verzeichnis.

   a Klicken Sie im Dialogfeld **[Check out (Auschecken)]** auf **[Options (Optionen)]** .

   b Klicken Sie neben dem Verzeichnis zum Auschecken auf **[Browse (Durchsuchen)]** und wählen Sie das Verzeichnis, das den Ordner mit dem Pool-Namen enthält.

      Wählen Sie nicht den Ordner mit dem Pool-Namen selbst aus.

      Wenn Sie z.B. Paketdateien für einen Pool mit dem Anzeigenamen `LocalPool` in das Verzeichnis `C:\CheckOutDirectory\LocalPool` kopiert haben, wählen Sie das Verzeichnis `C:\CheckOutDirectory`.

   c Klicken Sie auf **[OK]** .

4 Klicken Sie im Dialogfeld **[Check out (Auschecken)]** auf **[OK]** .

View Manager checkt den Desktop aus. View Transfer Server erkennt, dass sich die Basis-Image-Dateien auf dem Clientcomputer befinden und lädt nur die verbleibenden Desktop-Dateien herunter. Diese Dateien umfassen die Betriebssystemfestplatte und eine persistente Festplatte (sofern konfiguriert).

Fehlerbehebung bei View Transfer Server- und lokalen Desktop-Vorgängen

Tipps zur Fehlerbehebung sind für alle gängigen View Transfer Server- und lokalen Desktop-Vorgänge verfügbar.

- Auschecken schlägt mit Fehler „No Available Transfer Server (Kein Transfer Server verfügbar)“ fehl auf Seite 333

  Wenn Benutzer versuchen, ihre Desktops auszuchecken, schlägt der Vorgang fehl und die Fehlermeldung `No available Transfer Server (Kein Transfer Server verfügbar)` wird angezeigt.

- Probleme beim Auschecken des Desktops nach dem ersten Auschecken auf Seite 334

  Wenn View Transfer Server ordnungsgemäß funktioniert, kann der Grund für die Probleme beim Auschecken darin liegen, dass die View Connection Server-Instanz nicht mehr über den Verschlüsselungsschlüssel für Dateien auf dem lokalen Computer verfügt.

- Anmeldefenster wird erst sehr spät angezeigt auf Seite 334

  Unter bestimmten Umständen wird nach dem Öffnen von View Client und dem Angeben einer View Connection Server-Instanz das Anmeldefenster erst nach 30 oder mehr Sekunden angezeigt.

- View Transfer Server bleibt im Status „Pending (Ausstehend)“ auf Seite 335

  View Transfer Server ist nicht verfügbar, wenn er für eine ungewöhnlich lange Zeit im Status **[Pending (Ausstehend)]** bleibt. Dies gilt beispielsweise, wenn der Status **[Pending (Ausstehend)]** länger als zehn Minuten anhält.

- View Transfer Server wechselt nicht in den Wartungsmodus auf Seite 335

  Wenn Sie versuchen, View Transfer Server in den Wartungsmodus zu versetzen, bleibt dieser für eine ungewöhnlich lange Zeit im Status **[Maintenance mode pending (Wartungsmodus ausstehend)]** .

- Das Transfer Server-Repository ist ungültig auf Seite 336

  In View Administrator zeigt View Transfer Server den Status **[Bad Transfer Server repository (Ungültiges Transfer Server-Repository)]** an.

- View Transfer Server kann keine Verbindung zum Transfer Server-Repository herstellen auf Seite 336

  In View Administrator zeigt View Transfer Server den Status **[Repository Connection Error (Repository-Verbindungsfehler)]** an.

- Fehler bei Systemzustandsprüfung für View Transfer Server auf Seite 337

  In View Administrator zeigt View Transfer Server den Status **[Bad Transfer Server repository (Ungültiges Transfer Server-Repository)]** an. Im View Administrator-Dashboard wird View Transfer Server mit einem roten, nach unten zeigenden Pfeil angezeigt.

- Das Transfer Server-Repository fehlt auf Seite 337

  In View Administrator zeigt View Transfer Server den Status **[No Transfer Server Repository Configured (Kein Transfer Server-Repository konfiguriert)]** an.

- View Transfer Server-Instanzen weisen Konflikte mit Transfer Server-Repositorys auf auf Seite 338

  In View Administrator zeigt View Transfer Server den Status **[Transfer Server Repository Conflict (Transfer Server-Repository-Konflikt)]** an.

- Der View Transfer Server-Webdienst ist nicht verfügbar auf Seite 338

  In View Administrator zeigt View Transfer Server den Status **[Web Server Down (Webserver nicht aktiv)]** an.

- Die virtuelle Festplatte eines lokalen Desktops muss repariert werden auf Seite 339

  Sie müssen möglicherweise die virtuelle Festplatte eines lokalen Desktops reparieren.

- Wiederherstellen von Daten von einem lokalen Desktop auf Seite 339

  VMware View schützt die virtuelle Maschine eines lokalen Desktops, indem alle zugehörigen virtuellen Festplatten verschlüsselt werden. Wenn die ID für das Auschecken der virtuellen Maschine aus der Konfiguration gelöscht wird oder die Sitzungs- oder Richtliniendateien beschädigt werden, können Sie den lokalen Desktop möglicherweise nicht mehr einschalten oder einchecken. Sie können in diesem Fall die virtuelle Maschine des lokalen Desktops entschlüsseln, um Daten von ihm wiederherzustellen.

Auschecken schlägt mit Fehler „No Available Transfer Server (Kein Transfer Server verfügbar)“ fehl

Wenn Benutzer versuchen, ihre Desktops auszuchecken, schlägt der Vorgang fehl und die Fehlermeldung `No available Transfer Server (Kein Transfer Server verfügbar)` wird angezeigt.

Problem

Das Auschecken kann fehlschlagen, wenn der Vorgang zu etwa 10% abgeschlossen ist, bevor View Transfer Server mit dem Übertragen der Daten auf den Clientcomputer beginnt. Das Auschecken kann auch zu einem späteren Zeitpunkt fehlschlagen. Beispielsweise wird möglicherweise das Basis-Image auf den Clientcomputer übertragen, weitere Festplatten der virtuellen Maschine können jedoch nicht übertragen werden.

Dieses Problem tritt bei allen Auscheckvorgängen auf, die von einer bestimmten View Transfer Server-Instanz verwaltet werden.

Ursache

Dieses Problem kann auftreten, da View Transfer Server auf einem ESX-Host ausgeführt wird, der keinen Zugriff auf die Datenspeicher besitzt, in denen die Desktops enthalten sind. Während eines Auscheckvorgangs überträgt View Transfer Server Desktop-Daten von den Datenspeichern auf den Clientcomputer. Die Datenspeicher müssen von dem ESX-Host zugänglich sein, auf dem die virtuelle View Transfer Server-Maschine ausgeführt wird.

Lösung

- Migrieren Sie die virtuelle View Transfer Server-Maschine auf einen ESX-Host mit Zugriff auf die Datenspeicher.
  a Versetzen Sie in View Administrator die View Transfer Server-Instanz in den Wartungsmodus.
  b Verwenden Sie in vSphere Client den Migrations-Assistenten, um die virtuelle View Transfer Server-Maschine auf den Ziel-ESX-Host zu migrieren.
  c Wählen Sie in View Administrator die View Transfer Server-Instanz aus und beenden Sie den Wartungsmodus.
- Wenn Sie die virtuelle View Transfer Server-Maschine nicht migrieren können, erstellen Sie die View Transfer Server-Instanz auf einer anderen virtuellen Maschine auf einem ESX-Host neu, der Zugriff auf die Datenspeicher hat.
  a Entfernen Sie in View Administrator die View Transfer Server-Instanz aus View Manager.
  b Deinstallieren Sie in vSphere Client View Transfer Server oder entfernen Sie die virtuelle View Transfer Server-Maschine.
  c Erstellen Sie eine neue virtuelle Maschine auf dem Ziel-ESX-Host.
  d Installieren Sie View Transfer Server auf der virtuellen Maschine.
  e Fügen Sie in View Administrator View Transfer Server zu View Manager hinzu.

  Weitere Informationen zum Installieren von View Transfer Server finden Sie im Dokument *Installation von VMware View*.

Probleme beim Auschecken des Desktops nach dem ersten Auschecken

Wenn View Transfer Server ordnungsgemäß funktioniert, kann der Grund für die Probleme beim Auschecken darin liegen, dass die View Connection Server-Instanz nicht mehr über den Verschlüsselungsschlüssel für Dateien auf dem lokalen Computer verfügt.

Problem

Nachdem Sie einen lokalen Desktop erfolgreich aus- und wieder eingecheckt haben, kann beim erneuten Auschecken des Desktops keine Verbindung zum lokalen Desktop hergestellt werden. Möglicherweise wird Ihnen eine Fehlermeldung wie z.B `Cannot access local desktop – desktop is corrupted (Zugriff auf den lokalen Desktop ist nicht möglich – Desktop ist beschädigt)` angezeigt.

Ursache

Wenn Sie die Verschlüsselungsmethode für einen lokalen Desktop ändern oder den Desktop aus seinem Pool löschen und einen neuen Desktop erstellen, verwendet View Connection Server zum Generieren einer neuen Konfigurationsdatei einen neuen Authentifizierungsschlüssel.

Wenn Endbenutzer versuchen, den Desktop erneut auszuchecken, werden ausschließlich geänderte Dateien heruntergeladen. Für die neuen Dateien, die heruntergeladen werden, wird ein neuer Verschlüsselungsschlüssel verwendet. Hingegen wird für die alten Dateien, die sich bereits auf dem lokalen Computer befinden, der alte Verschlüsselungsschlüssel verwendet, über den View Connection Server nicht mehr verfügt.

Lösung

- Endbenutzer müssen alle lokalen Desktop-Dateien löschen, bevor Sie den Desktop erneut auschecken.

  Der Ordner befindet sich im Auscheckverzeichnis des lokalen Desktops. Wenn Sie beim ersten Herunterladen des Desktops nicht auf **[Options (Optionen)]** geklickt und das Verzeichnis zur Speicherung der lokalen Desktops geändert haben, werden lokale Desktops im Standardverzeichnis für das Auschecken gespeichert.

Desktop-Betriebssystem	Standardverzeichnis für das Auschecken
Standardverzeichnis unter Windows 7 und Windows Vista	`C:\Benutzer\`*`Benutzername`*`\AppData\Local\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*
Standardverzeichnis unter Windows XP	`C:\Dokumente und Einstellungen\`*`Benutzername`*`\Lokale Einstellungen\Anwendungsdaten\VMware\VDM\Local Desktops\`*`Anzeigename_des_Pools`*

Anmeldefenster wird erst sehr spät angezeigt

Unter bestimmten Umständen wird nach dem Öffnen von View Client und dem Angeben einer View Connection Server-Instanz das Anmeldefenster erst nach 30 oder mehr Sekunden angezeigt.

Problem

Das Anmeldefenster ist gelegentlich für 30 Sekunden nicht verfügbar, bis eine Zeitüberschreitung für die Verbindung auftritt.

Ursache

Wenn View Client eine IP-Adresse für View Connection Server verwendet, tritt dieses Problem auf, wenn Sie über eine Netzwerkverbindung verfügen, jedoch keine View Connection Server-Instanz erreichbar ist. Beispielsweise kann dieses Problem auftreten, wenn Sie versuchen, sich von zu Hause aus an einem lokalen Desktop anzumelden und zwar eine Internetverbindung verfügbar ist, jedoch keine VPN-Verbindung, die Zugriff auf View Connection Server ermöglicht.

Wenn View Client in einem LAN anstelle einer IP-Adresse einen Hostnamen verwendet, wird dieses Problem dadurch verursacht, dass View Connection Server (oder bei Verwendung eines Proxys der Proxy) nicht verfügbar ist oder eine Firewall die Verbindung blockiert. In einem WAN tritt dieses Problem aus den gleichen Gründen auf. Eine weitere Ursache könnte jedoch sein, dass der Hostname im öffentlichen DNS auflösbar ist, auf den Server jedoch nicht über das WAN zugegriffen werden kann.

Lösung

Sie müssen warten, bis eine Zeitüberschreitung für den Verbindungsversuch auftritt. Das Anmeldefenster wird schließlich angezeigt.

View Transfer Server bleibt im Status „Pending (Ausstehend)“

View Transfer Server ist nicht verfügbar, wenn er für eine ungewöhnlich lange Zeit im Status **[Pending (Ausstehend)]** bleibt. Dies gilt beispielsweise, wenn der Status **[Pending (Ausstehend)]** länger als zehn Minuten anhält.

Problem

Nachdem Sie View Transfer Server zu View Manager hinzugefügt haben, wechselt der Status von View Transfer Server nicht in den Status **[Ready (Bereit)]** .

Ursache

Eine häufige Ursache dafür ist, dass die View Connection Server-Instanz keine Verbindung zu View Transfer Server herstellen kann.

Lösung

- Stellen Sie sicher, dass View Transfer Server auf der virtuellen Maschine installiert ist.
- Stellen Sie sicher, dass die View Transfer Server-Dienste ausgeführt werden.
  a Öffnen Sie auf der virtuellen View Transfer Server-Maschine das Dialogfeld **[Control Panel (Systemsteuerung)] > [Administrative Tools (Verwaltung)] > [Services (Dienste)]** .
  b Stellen Sie sicher, dass VMware View Transfer Server-Dienst, VMware View Transfer Server-Steuerungsdienst und die VMware View-Framework-Komponentendienste gestartet wurden.
- Stellen Sie sicher, dass die virtuelle View Transfer Server-Maschine den View Connection Server-Hostnamen auflösen kann.
- Stellen Sie sicher, dass der Connection Server-Computer ein Ping-Signal an die IP-Adresse der View Transfer Server-Instanz senden kann.
- Stellen Sie sicher, dass die virtuelle View Transfer Server-Maschine der empfohlenen Systemkonfiguration entspricht. Informationen zu den View Transfer Server-Systemanforderungen finden Sie im Dokument *Installation von VMware View*.

View Transfer Server wechselt nicht in den Wartungsmodus

Wenn Sie versuchen, View Transfer Server in den Wartungsmodus zu versetzen, bleibt dieser für eine ungewöhnlich lange Zeit im Status **[Maintenance mode pending (Wartungsmodus ausstehend)]** .

Problem

Wenn sich View Transfer Server im Status **[Maintenance mode pending (Wartungsmodus ausstehend)]** befindet, können Sie keine Vorgänge wie das Migrieren des Transfer Server-Repositorys auf einen neuen Speicherort durchführen. Die ist erst möglich, wenn View Transfer Server in den Wartungsmodus gewechselt hat.

Ursache

Aktive Übertragungs- oder Paketveröffentlichungsvorgänge in das Transfer Server-Repository sind noch nicht abgeschlossen.

Lösung

Warten Sie, bis die aktiven Datenübertragungs- oder Veröffentlichungsvorgänge abgeschlossen sind. View Transfer Server wechselt in den Wartungsmodus, wenn alle Vorgänge abgeschlossen sind.

Das Transfer Server-Repository ist ungültig

In View Administrator zeigt View Transfer Server den Status **[Bad Transfer Server repository (Ungültiges Transfer Server-Repository)]** an.

Problem

Solange sich View Transfer Server in diesem Status befindet, können Sie weder Übertragungsvorgänge für Linked-Clone-Desktops ausführen noch Pakete veröffentlichen.

Ursache

Das Transfer Server-Repository, mit dem sich View Transfer Server entsprechend der Konfiguration verbindet, unterscheidet sich von dem Transfer Server-Repository, das derzeit in der View Connection Server-Instanz konfiguriert ist.

Eine ungültige Migration des Transfer Server-Repositorys kann dazu führen, dass View Transfer Server in diesen Status wechselt.

Lösung

Erneutes Migrieren des Transfer Server-Repositorys an einen neuen Speicherort. Anweisungen finden Sie unter „Migrieren des Transfer Server-Repositorys an einen neuen Speicherort“, auf Seite 306.

View Transfer Server kann keine Verbindung zum Transfer Server-Repository herstellen

In View Administrator zeigt View Transfer Server den Status **[Repository Connection Error (Repository-Verbindungsfehler)]** an.

Problem

View Transfer Server kann keine Verbindung zum Transfer Server-Repository herstellen, das in View Connection Server konfiguriert ist.

Ursache

Die Konfiguration des Transfer Server-Repository ist ungültig. Wenn das Repository auf einer Netzwerkfreigabe konfiguriert ist, sind Netzwerkpfad oder Anmeldeinformationen ungültig. Wenn es sich um ein lokales Repository handelt, ist der Dateisystempfad ungültig.

Lösung

1 Versetzen Sie alle View Transfer Server-Instanzen in den Wartungsmodus.

   a Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

   b Wählen Sie eine View Transfer Server-Instanz aus.

   c Finden gerade Übertragungen statt, müssen Sie entweder die aktiven Übertragungen abbrechen oder warten, bis die aktiven Übertragungen abgeschlossen sind, bevor Sie die View Transfer Server-Instanz in den Wartungsmodus versetzen.

d Klicken Sie auf **[OK]** .

e Wiederholen Sie diese Schritte für alle View Transfer Server-Instanzen.

2 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

3 Klicken Sie auf **[Edit (Bearbeiten)]** und konfigurieren Sie das Transfer Server-Repository neu.

View Transfer Server überprüft das Transfer Server-Repository auf Gültigkeit.

Fehler bei Systemzustandsprüfung für View Transfer Server

In View Administrator zeigt View Transfer Server den Status **[Bad Transfer Server repository (Ungültiges Transfer Server-Repository)]** an. Im View Administrator-Dashboard wird View Transfer Server mit einem roten, nach unten zeigenden Pfeil angezeigt.

Problem

Im Zustand **[Bad Health Check (Fehler bei Systemzustandsprüfung)]** funktioniert View Transfer Server nicht ordnungsgemäß. Sie können im Transfer Server-Repository weder Übertragungsvorgänge ausführen noch Pakete veröffentlichen.

Ursache

View Transfer Server ist nicht verfügbar, wird nicht ausgeführt oder funktioniert nicht ordnungsgemäß.

Lösung

- Stellen Sie sicher, dass View Transfer Server auf der virtuellen Maschine installiert ist.
- Stellen Sie sicher, dass die View Transfer Server-Dienste ausgeführt werden.
  a Öffnen Sie auf der virtuellen View Transfer Server-Maschine das Dialogfeld **[Control Panel (Systemsteuerung)] > [Administrative Tools (Verwaltung)] > [Services (Dienste)]** .
  b Stellen Sie sicher, dass VMware View Transfer Server-Dienst, VMware View Transfer Server-Steuerungsdienst und die VMware View-Framework-Komponentendienste gestartet wurden.
- Stellen Sie sicher, dass die virtuelle View Transfer Server-Maschine den View Connection Server-Hostnamen auflösen kann.
- Stellen Sie sicher, dass der Connection Server-Computer ein Ping-Signal an die IP-Adresse der View Transfer Server-Instanz senden kann.
- Stellen Sie sicher, dass die virtuelle View Transfer Server-Maschine der empfohlenen Systemkonfiguration entspricht. Informationen zu den View Transfer Server-Systemanforderungen finden Sie im *VMware View-Installationshandbuch*.

Das Transfer Server-Repository fehlt

In View Administrator zeigt View Transfer Server den Status **[No Transfer Server Repository Configured (Kein Transfer Server-Repository konfiguriert)]** an.

Problem

Sie können weder Übertragungsvorgänge für Linked-Clone-Desktops ausführen noch Pakete im View Transfer Server-Repository veröffentlichen.

Ursache

In View Manager ist kein Transfer Server-Repository konfiguriert.

Lösung

1 Versetzen Sie alle View Transfer Server-Instanzen in den Wartungsmodus.

   a Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

   b Wählen Sie eine View Transfer Server-Instanz aus.

   c Finden gerade Übertragungen statt, müssen Sie entweder die aktiven Übertragungen abbrechen oder warten, bis die aktiven Übertragungen abgeschlossen sind, bevor Sie die View Transfer Server-Instanz in den Wartungsmodus versetzen.

   d Klicken Sie auf **[OK]** .

   e Wiederholen Sie diese Schritte für alle View Transfer Server-Instanzen.

2 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Transfer Server-Repository]** .

3 Klicken Sie auf **[Edit (Bearbeiten)]** und konfigurieren Sie das Transfer Server-Repository.

   View Transfer Server überprüft das Transfer Server-Repository auf Gültigkeit.

View Transfer Server-Instanzen weisen Konflikte mit Transfer Server-Repositorys auf

In View Administrator zeigt View Transfer Server den Status **[Transfer Server Repository Conflict (Transfer Server-Repository-Konflikt)]** an.

Problem

Sie können weder Übertragungsvorgänge für Linked-Clone-Desktops ausführen noch Pakete im View Transfer Server-Repository veröffentlichen.

Ursache

Mehrere View Transfer Server-Instanzen sind für die Verbindung mit verschiedenen Transfer Server-Repositorys konfiguriert.

Dieser Status kann auftreten, wenn gleichzeitig mehrere View Transfer Server-Instanzen zu View Manager hinzugefügt werden und jede Instanz mit einem anderen Transfer Server-Repository konfiguriert wird.

Lösung

Entfernen Sie die View Transfer Server-Instanzen aus View Manager und fügen Sie eine nach der anderen wieder hinzu. Wenn eine View Transfer Server-Instanz den Status **[Bad Transfer Server Repository (Ungültiges Transfer Server-Repository)]** anzeigt, finden Sie Informationen zur Fehlerbehebung unter „Das Transfer Server-Repository ist ungültig“, auf Seite 336.

Der View Transfer Server-Webdienst ist nicht verfügbar

In View Administrator zeigt View Transfer Server den Status **[Web Server Down (Webserver nicht aktiv)]** an.

Problem

View Transfer Server kann keine Pakete aus dem Transfer Server-Repository herunterladen und keine anderen Desktop-Daten an lokale Desktops übertragen.

Ursache

Der Apache2.2-Webdienst, der das Transfer Server-Repository unterstützt, wird nicht ausgeführt.

Lösung

1 Öffnen Sie auf der virtuellen View Transfer Server-Maschine das Dialogfeld **[Control Panel (Systemsteuerung)] > [Administrative Tools (Verwaltung)] > [Services (Dienste)]** .

2 Starten Sie den Apache2.2-Dienst.

Die virtuelle Festplatte eines lokalen Desktops muss repariert werden

Sie müssen möglicherweise die virtuelle Festplatte eines lokalen Desktops reparieren.

Problem

Wenn Sie versuchen, eine Verbindung zum lokalen Desktop herzustellen, wird eine Fehlermeldung angezeigt. Beispiel:

```
Datenträger 'C:\Dokumente und Einstellungen\jo\Lokale Einstellungen\Anwendungsdaten\View\Local
Desktops\Win7_32b_Local_Mode\52411f5e05b854ca-b5c54521f6010b22-scsi00-000002.vmdk' oder ein
Snapshot, von dem er abhängt, kann nicht geöffnet werden.

Ursache: Die angegebene virtuelle Festplatte muss repariert werden.
```

Ursache

Das Problem kann auftreten, wenn Sie den Clientcomputer trennen oder ausschalten, während das Image der virtuellen Datei aktualisiert wird.

Lösung

1 Starten Sie View Client von der Befehlszeile, indem Sie die Option `–repairLocalDesktops` angeben.

Beispiel:

```
wswc –desktopName lmdt01 –userName jo –domainName MYDOM –repairLocalDesktops
```

Der Reparaturvorgang kann mehrere Minuten in Anspruch nehmen.

2 Sollte die Reparatur fehlschlagen, führen Sie ein Rollback der lokalen Sitzung durch und checken Sie einen neuen lokalen Desktop aus.

Wiederherstellen von Daten von einem lokalen Desktop

VMware View schützt die virtuelle Maschine eines lokalen Desktops, indem alle zugehörigen virtuellen Festplatten verschlüsselt werden. Wenn die ID für das Auschecken der virtuellen Maschine aus der Konfiguration gelöscht wird oder die Sitzungs- oder Richtliniendateien beschädigt werden, können Sie den lokalen Desktop möglicherweise nicht mehr einschalten oder einchecken. Sie können in diesem Fall die virtuelle Maschine des lokalen Desktops entschlüsseln, um Daten von ihm wiederherzustellen.

WICHTIG Nutzen Sie dieses Verfahren nur, wenn die Daten in einem lokalen Desktop nicht mit einer anderen Methode wiederhergestellt werden können.

Die View Connection Server-Instanz muss auf die View LDAP-Konfiguration zugreifen können, die den Authentifizierungsschlüssel für den lokalen Desktop enthält.

Je nachdem, wie viele Daten Sie wiederherstellen möchten, können Sie entweder die vollständige virtuelle Maschine oder lediglich eine der zugehörigen Festplatten entschlüsseln. Die Entschlüsselung erfolgt schneller, wenn nur eine einzelne Festplatte entschlüsselt wird.

Voraussetzungen

- Stellen Sie sicher, dass für den lokalen Desktop kein Rollback ohne Datenverlust durchgeführt werden kann.

- Stellen Sie sicher, dass die Daten im lokalen Desktop weder repliziert noch an einem anderen Speicherort gespeichert wurden.
- Melden Sie sich als ein Benutzer mit der Rolle **Administrators (Administratoren)** auf dem Windows-Computer an, auf dem die View Connection Server-Instanz installiert ist.
- Stellen Sie sicher, dass der Ordner, in dem Sie die Entschlüsselung durchführen möchten, über ausreichend Speicherplatz zur Aufnahme der verschlüsselten und der entschlüsselten Dateien der virtuellen Maschine verfügt, und dass Sie Schreibberechtigungen für diesen Ordner besitzen.

Vorgehensweise

1 Kopieren Sie die Dateien der virtuellen Maschine vom Clientcomputer in einen lokalen Ordner auf der View Connection Server-Instanz.

WICHTIG Greifen Sie nicht über eine Netzwerkfreigabe oder ein zugeordnetes Laufwerk auf die Dateien zu.

2 Führen Sie zum Entschlüsseln einer Datei den Befehl `vdmadmin` aus.

```
vdmadmin –V –rescue –d Desktop –u Domäne\Benutzer –infile Pfad_zu_VM–Datei
```

Option	Beschreibung
–d *Desktop*	Legt den Namen des Desktop-Pools fest.
–infile *Pfad_zu_VM-Datei*	Gibt den Pfad zur VM-Datei der virtuellen Maschine für den lokalen Desktop an. Zum Wiederherstellen einer vollständigen virtuellen Maschine geben Sie den Namen der Konfigurationsdatei für die virtuelle VMware-Maschine (VMX-Datei) als Argument der Option `–infile` an. Zum Wiederherstellen einer einzelnen Festplatte einer virtuellen Maschine geben Sie den Namen der virtuellen VMware-Festplattendatei (VMDK-Datei) als Argument der Option `–infile` an. Geben Sie keine VMDK-Datei an, die einem Festplatten-Slice entspricht.
–u *Domäne\Benutzer*	Gibt die Domäne und den Namen des Endbenutzers für den lokalen Desktop an.

Der Befehl `vdmadmin` schreibt die entschlüsselten Dateien der virtuellen Maschine in einen Unterordner namens `rescued`.

Beispiel: Entschlüsseln der Dateien einer virtuellen Maschine

Entschlüsseln Sie eine vollständige virtuelle Maschine durch Angeben der zugehörigen VMX-Datei.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile "J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Appli–
cations,DC=mycorp,DC=com.vmx"
```

Listen Sie die Dateien auf, die für die Festplatte `scsi00` der virtuellen Maschine für einen lokalen Desktop verfügbar sind.

```
J:\Temp\LMDT_Recovery>dir /b *scsi00*
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s002.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s003.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s004.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s001.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s002.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s003.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s004.vmdk
```

Entschlüsseln Sie die aktuelle Version der Festplatte `scsi00` durch Angeben der zugehörigen VMDK-Datei.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile "J:\Temp\LMDT_Reco–
very\52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk"
```

Weiter

Verwenden Sie VMware Workstation zum Einschalten und Überprüfen einer entschlüsselten vollständigen virtuellen Maschine, oder VMware DiskMount zum Mounten einer entschlüsselten Festplatte. Alternativ können Sie die Inhalte einer entschlüsselten Festplatte überprüfen, indem Sie die zugehörige VMDK-Datei an eine virtuelle Maschine in VMware Workstation. Wenn Sie die Daten der Dateien einer virtuellen Maschine wiederhergestellt haben, führen Sie ein Rollback für den lokalen Desktop durch.

Warten von View-Komponenten 15

Um die Verfügbarkeit und den fehlerfreien Betrieb Ihrer View Manager-Komponenten sicherzustellen, können Sie verschiedene Wartungsaufgaben ausführen.

Dieses Kapitel behandelt die folgenden Themen:

- „Sichern und Wiederherstellen von View-Konfigurationsdaten“, auf Seite 343
- „Überwachen von View-Komponenten“, auf Seite 349
- „Überwachen des Desktop-Status“, auf Seite 349
- „Grundlegendes zu den View Manager-Diensten“, auf Seite 350
- „Hinzufügen von Lizenzen zu VMware View“, auf Seite 352
- „Aktualisieren allgemeiner Benutzerinformationen aus Active Directory“, auf Seite 353
- „Migrieren von View Composer mit einer vorhandenen Datenbank“, auf Seite 353
- „Aktualisieren der Zertifikate auf einer View Connection Server-Instanz oder einem Sicherheitsserver“, auf Seite 355

Sichern und Wiederherstellen von View-Konfigurationsdaten

Sie können Ihre View Manager- und View Composer-Konfigurationsdaten sichern, indem Sie in View Administrator automatische Sicherungen planen oder ausführen. Sie können Ihre View-Konfiguration wiederherstellen, indem Sie die gesicherten View LDAP-Dateien und View Composer-Datenbankdateien manuell importieren.

Sie können die Sicherungs- und Wiederherstellungsfunktionen verwenden, um View-Konfigurationsdaten beizubehalten und zu migrieren.

Sichern von View Connection Server- und View Composer-Daten

Nachdem Sie die anfängliche Konfiguration von View Connection Server abgeschlossen haben, sollten Sie regelmäßige Sicherungen Ihrer View Manager- und View Composer-Konfigurationsdaten planen. Sie können Ihre View Manager- und View Composer-Daten mithilfe von View Administrator sichern.

View Manager speichert View Connection Server-Konfigurationsdaten im View LDAP-Repository. View Composer speichert Konfigurationsdaten für Linked-Clone-Desktops in der View Composer-Datenbank.

Wenn Sie Sicherungen mithilfe von View Administrator durchführen, sichert View Manager die View LDAP-Konfigurationsdaten und die View Composer-Datenbank. Beide Sicherungsdateisätze werden am selben Speicherort abgelegt. Die View LDAP-Daten werden im LDAP Data Interchange Format (LDIF) exportiert. Eine Beschreibung von View LDAP finden Sie unter „View LDAP-Verzeichnis“, auf Seite 25.

View Manager kann Konfigurationsdaten aus einer beliebigen View Connection Server-Instanz exportieren.

Wenn mehrere View Connection Server-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren. Alle replizierten Instanzen umfassen dieselben Konfigurationsdaten.

Verlassen Sie sich nicht darauf, dass replizierte Instanzen von View Connection Server als Sicherungsmechanismus fungieren. Wenn View Manager Daten in replizierten Instanzen von View Connection Server synchronisiert, werden die auf einer Instanz verlorenen Daten bei der Datenharmonisierung von allen Mitgliedern der replizierten Gruppe entfernt.

Wenn View Connection Server mehrere vCenter Server-Instanzen mit mehreren View Composer-Diensten verwendet, sichert View Manager alle mit sämtlichen vCenter Server-Instanzen verknüpften View Composer-Datenbanken.

Sie können Sicherungen auf verschiedene Arten ausführen.

- Planen Sie automatische Sicherungen unter Verwendung der View Manager-Funktion für die Konfigurationssicherung.
- Wenn Sie sofort eine Sicherung durchführen möchten, verwenden Sie die Funktion **[Backup Now (Jetzt sichern)]** in View Administrator.
- Einen manuellen Export der View LDAP-Daten können Sie mit dem Tool `vdmexport` durchführen. Dieses Tool wird mit jeder Instanz von View Connection Server bereitgestellt.

Hinweis Das Tool `vdmexport` sichert nur die View LDAP-Daten. Mit diesem Tool werden keine View Composer-Datenbankinformationen gesichert.

Planen von View Manager-Konfigurationssicherungen

Sie können die Sicherung Ihrer View Manager-Konfigurationsdaten planen, sodass die Daten in regelmäßigen Abständen gesichert werden. View Manager sichert die Inhalte des View LDAP-Repository, in dem die View Connection Server-Instanzen ihre Konfigurationsdaten speichern.

Sie können die Konfigurationsdateien sofort sichern, indem Sie die View Connection Server-Instanz auswählen und auf **[Backup Now (Jetzt sichern)]** klicken.

Voraussetzungen

Machen Sie sich mit den Sicherungseinstellungen vertraut. Siehe „Einstellungen für die View Manager-Konfigurationssicherung“, auf Seite 345.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Configuration (Konfiguration)]** > **[Servers (Server)]** .

2 Wählen Sie die zu sichernde View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Geben Sie die Einstellungen für die View Manager-Konfigurationssicherung an. Legen Sie beispielsweise die Sicherungshäufigkeit, die Anzahl an Sicherungsdateien sowie den Speicherort für die Sicherungsdateien fest.

4 Klicken Sie auf **[OK]** .

Einstellungen für die View Manager-Konfigurationssicherung

View Manager kann Ihre View Connection Server- und View Composer-Konfigurationsdaten in regelmäßigen Abständen sichern. In View Administrator können Sie die Häufigkeit und andere Aspekte der Sicherungsvorgänge festlegen.

Tabelle 15-1. Einstellungen für die View Manager-Konfigurationssicherung

Einstellung	Beschreibung
Automatic backup frequency (Häufigkeit für automatische Sicherungen)	Jede Stunde. Sicherungen werden einmal pro Stunde zur vollen Stunde erstellt. Alle 6 Stunden. Sicherungen werden um 24:00 Uhr, 6:00 Uhr, 12:00 Uhr und 18:00 erstellt. Alle 12 Stunden. Sicherungen werden um 24:00 Uhr und um 12:00 Uhr erstellt. Jeden Tag. Sicherungen werden einmal pro Tag um 24:00 Uhr erstellt. Alle 2 Tage. Sicherungen werden am Samstag, Montag, Mittwoch und Freitag jeweils um 24:00 Uhr erstellt. Jede Woche. Sicherungen werden einmal pro Woche am Samstag um 24:00 Uhr erstellt. Alle 2 Wochen. Sicherungen werden jede zweite Woche am Samstag um 24:00 Uhr erstellt. Nie. Es werden keine automatischen Sicherungen ausgeführt.
Max number of backups (Maximale Anzahl an Sicherungen)	Gibt die Anzahl an Sicherungsdateien an, die auf der View Connection Server-Instanz gespeichert werden können. Bei dem hier angegebenen Wert muss es sich um eine Ganzzahl handeln, die größer ist als 0. Wird der angegebene Wert erreicht, wird die älteste Sicherungsdatei von View Manager gelöscht. Diese Einstellung gilt auch für Sicherungsdateien, die mit der Option **[Backup Now (Jetzt sichern)]** erstellt werden.
Folder Location (Speicherort für Ordner)	Gibt den Speicherort für die Sicherungsdateien an. Der standardmäßige Speicherort ist der folgende Pfad auf dem Computer, auf dem View Connection Server ausgeführt wird. ■ Auf einem Windows Server 2008-Computer: `C:\ProgramData\VMWare\VDM\backups` ■ Auf einem Windows Server 2003-Computer: `C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\backups` Bei Verwendung der Option **[Backup Now (Jetzt sichern)]** legt View Manager die Sicherungsdateien ebenfalls an diesem Speicherort ab.

Exportieren von Konfigurationsdaten aus View Connection Server

Sie können die Konfigurationsdaten einer View Connection Server-Instanz sichern, indem Sie die Inhalte des zugehörigen View LDAP-Repository exportieren.

Verwenden Sie den Befehl `vdmexport`, um die Daten in eine LDIF-Datei zu exportieren. Sie können den Befehl `vdmexport` auf einer beliebigen View Connection Server-Instanz ausführen.

Wenn mehrere View Connection Server-Instanzen in einer replizierten Gruppe vorhanden sind, müssen Sie die Daten nur aus einer Instanz exportieren. Alle replizierten Instanzen umfassen dieselben Konfigurationsdaten.

Hinweis Der Befehl `vdmexport.exe` sichert nur die View LDAP-Daten. Mit diesem Befehl werden keine View Composer-Datenbankinformationen gesichert.

Voraussetzungen

- Suchen Sie im folgenden Standardpfad nach der ausführbaren Datei `vdmexport.exe`, die zusammen mit View Connection Server installiert wird.

  ```
  C:\Programme\VMware\VMware View\Server\tools\bin
  ```

- Melden Sie sich an einer View Connection Server-Instanz als Benutzer mit der Rolle **[Administrators (Administratoren)]** oder **[Administrators (Read only) (Administratoren (Nur Lesen))]** an.

Vorgehensweise

1 Wählen Sie **[Start]** > **[Command Prompt (Eingabeaufforderung)]** .

2 Geben Sie an der Eingabeaufforderung den Befehl `vdmexport` ein und leiten Sie die Ausgabe in eine Datei um.

Beispiel:

```
vdmexport > MeinExport.LDF
```

Sie können den Namen der Ausgabedatei als Argument für den Parameter `–f` festlegen.

Beispiel:

```
vdmexport –f MeinExport.LDF
```

Der Befehl `vdmexport` schreibt die View Connection Server-Konfigurationsdaten in die angegebene LDIF-Datei.

Weitere Informationen zum Befehl `vdmexport` finden Sie im Dokument *Integration von VMware View*.

Weiter

Sie können die LDIF-Datei zum Ausführen der folgenden Verwaltungsaufgaben in Bezug auf Ihre Konfigurationsdaten verwenden:

- Wiederherstellen oder Übertragen der Konfigurationsdateien von View Connection Server.
- Ändern der Konfigurationsinformationen von View Connection Server durch Bearbeiten der Einträge der Datei und anschließendes Importieren der Datei auf die View Connection Server-Zielinstanz.

Weitere Informationen zum Importieren der LDIF-Datei finden Sie unter „Wiederherstellen von View Connection Server- und View Composer-Konfigurationsdaten“, auf Seite 346.

Wiederherstellen von View Connection Server- und View Composer-Konfigurationsdaten

Sie können die von View Manager gesicherten View Connection Server-LDAP-Konfigurationsdateien und die View Composer-Datenbankdateien manuell wiederherstellen.

Sie führen manuell verschiedene Dienstprogramme aus, um die View Connection Server- und View Composer-Konfigurationsdateien wiederherzustellen.

Bevor Sie Konfigurationsdaten wiederherstellen, sollten Sie sicherstellen, dass Sie die Konfigurationsdaten in View Administrator gesichert haben. Siehe „Sichern von View Connection Server- und View Composer-Daten“, auf Seite 343.

Verwenden Sie das Dienstprogramm `vdmimport`, um die View Connection Server-Daten aus den LDIF-Sicherungsdateien in das View LDAP-Repository der View Connection Server-Instanz zu importieren.

Mit dem Dienstprogramm `SviConfig` können Sie die View Composer-Daten aus den `.svi`-Sicherungsdateien in die View Composer-SQL-Datenbank importieren.

Importieren von Konfigurationsdaten in View Connection Server

Sie können die Konfigurationsdaten einer View Connection Server-Instanz wiederherstellen, indem Sie eine Sicherungskopie der in einer LDIF-Datei gespeicherten Daten importieren.

Verwenden Sie den Befehl `vdmimport`, um die Daten aus der LDIF-Datei in das View LDAP-Repository der View Connection Server-Instanz zu importieren.

Informationen zum Sichern des View LDAP-Repository finden Sie unter „Sichern von View Connection Server- und View Composer-Daten“, auf Seite 343.

Voraussetzungen

- Suchen Sie im folgenden Standardpfad nach der ausführbaren Datei `vdmimport`, die zusammen mit View Connection Server installiert wird.

  ```
  C:\Programme\VMware\VMware View\Server\tools\bin
  ```

- Melden Sie sich an einer View Connection Server-Instanz als Benutzer mit der Rolle **[Administrators (Administratoren)]** an.

Vorgehensweise

1 Wählen Sie **[Start] > [Command Prompt (Eingabeaufforderung)]** .

2 Geben Sie an der Eingabeaufforderung den Befehl `vdmimport` ein und legen Sie eine vorhandene LDIF-Datei als Argument für den Parameter `–f` fest.

  Beispiel:

  ```
  vdmimport –f MeinExport.LDF
  ```

Der Befehl `vdmimport` aktualisiert das View LDAP-Repository in View Connection Server mit den Konfigurationsdaten aus der LDIF-Datei.

Weitere Informationen zum Befehl `vdmimport` finden Sie im Dokument *Integration von VMware View*.

Wiederherstellen einer View Composer-Datenbank

Sie können die Sicherungsdateien für Ihre View Composer-Konfiguration in die View Composer-Datenbank importieren, die Linked-Clone-Informationen speichert.

Mithilfe des Befehls `SviConfig restoredata` können Sie die View Composer-Datenbank nach einem Systemausfall wiederherstellen oder die View Composer-Konfiguration in einen früheren Zustand zurückversetzen.

Wichtig Nur erfahrene View Composer-Administratoren sollten das Dienstprogramm `SviConfig` verwenden. Mit diesem Dienstprogramm lassen sich Fehler im Zusammenhang mit dem View Composer-Dienst behandeln.

Voraussetzungen

Ermitteln Sie den Speicherort der Sicherungsdateien für die View Composer-Datenbank. Standardmäßig speichert View Manager die Sicherungsdateien auf Laufwerk `C:` des View Connection Server-Computers:

- Auf einem Windows Server 2008-Computer: `C:\ProgramData\VMWare\VDM\backups`
- Auf einem Windows Server 2003-Computer: `C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VDM\backups`

View Composer-Sicherungsdateien folgen einer Namenskonvention mit Datumsstempel und `.svi`-Suffix.

`Backup–`*`Jahr_Monat_Tag_Nummer–vCenter Server–Name_Domänenname`*`.svi`

Beispiel: `Backup–20090304000010–foobar_test_org.svi`

Vorgehensweise

1 Kopieren Sie die View Composer-Sicherungsdateien vom View Connection Server-Computer an einen Speicherort, auf den vom vCenter Server-Computer zugegriffen werden kann, auf dem der View Composer-Dienst installiert ist.

2 Beenden Sie auf dem vCenter Server-Computer den VMware View Composer-Dienst.

3 Öffnen Sie auf dem vCenter Server-Computer eine Windows-Eingabeaufforderung und navigieren Sie zu der ausführbaren Datei `SviConfig`.

Die Datei befindet sich im Ordner der View Composer-Anwendung.

```
C:\Programme\VMware\VMware View Composer\sviconfig.exe
```

4 Führen Sie den Befehl `SviConfig restoredata` aus.

```
sviconfig –operation=restoredata
                  –DsnName=Ziel–DSN (Database Source Name)
                  –Username=Benutzername_Datenbankadministrator
                  –Password=Kennwort_Datenbankadministrator
                  –BackupFilePath=Pfad_zu_View Composer–Sicherungsdatei
```

Beispiel:

```
sviconfig –operation=restoredata –dsnname=LinkedClone
–username=Admin –password=Pass
–backupfilepath="C:\Programme\VMware\VMware View
Composer\Backup–20090304000010–foobar_test_org.SVI"
```

5 Starten Sie den VMware View Composer-Dienst.

Weiter

Ergebniscodes zur Ausgabe des Befehls `SviConfig restoredata` finden Sie unter „Ergebniscodes für das Wiederherstellen der View Composer-Datenbank“, auf Seite 348.

Ergebniscodes für das Wiederherstellen der View Composer-Datenbank

Wenn Sie eine View Composer-Datenbank wiederherstellen, zeigt der Befehl `SviConfig restoredata` einen Ergebniscode an.

Tabelle 15-2. Restoredata-Ergebniscodes

Code	Beschreibung
0	Vorgang erfolgreich abgeschlossen.
1	Angegebener DSN wurde nicht gefunden.
2	Angegebene Anmeldeinformationen für Datenbankadministrator sind ungültig.
3	Treiber für die Datenbank wird nicht unterstützt.
4	Unerwartetes Problem ist aufgetreten und der Befehl konnte nicht abgeschlossen werden.
14	View Composer-Dienst wird von einer anderen Anwendung verwendet. Beenden Sie den Dienst, bevor Sie den Befehl ausführen.
15	Während des Wiederherstellungsvorgangs ist ein Problem aufgetreten. Einzelheiten sind in der angezeigten Protokollausgabe aufgeführt.

Überwachen von View-Komponenten

Sie können den Status der View Manager- und vSphere-Komponenten in Ihrer View-Bereitstellung problemlos über das View Administrator-Dashboard überwachen.

View Administrator zeigt Überwachungsinformationen zu View Connection Server-Instanzen, der Ereignisdatenbank, zu Sicherheitsservern, View Composer-Diensten, Datenspeichern, vCenter Server-Instanzen und Domänen an.

Hinweis View Manager kann keine Statusinformationen zu Kerberos-Domänen sammeln. View Administrator zeigt den Status von Kerberos-Domänen als unbekannt an, selbst wenn eine Domäne konfiguriert wurde und fehlerfrei arbeitet.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Dashboard]** .

2 Erweitern Sie im Fensterbereich **[System Health (Systemzustand)]** die Einträge **[View components (View-Komponenten)]** , **[vSphere components (vSphere-Komponenten)]** oder **[Other components (Andere Komponenten)]** .

- Ein grüner, nach oben weisender Pfeil weist darauf hin, dass für eine Komponente keine Probleme vorliegen.
- Ein roter, nach unten weisender Pfeil weist darauf hin, dass eine Komponente nicht verfügbar ist oder nicht funktioniert.
- Ein gelber Doppelpfeil weist darauf hin, dass sich eine Komponente in einem Warnzustand befindet.
- Ein Fragezeichen weist darauf hin, dass der Status einer Komponente unbekannt ist.

3 Klicken Sie auf einen Komponentennamen.

In einem Dialogfeld werden Name, Version, Status und weitere Informationen zur Komponente angezeigt.

Überwachen des Desktop-Status

Sie können den Status von Desktops in einer View-Bereitstellung problemlos über das View Administrator-Dashboard überwachen. Beispielsweise können alle getrennten Desktops oder alle Desktops im Wartungsmodus angezeigt werden.

Voraussetzungen

Machen Sie sich mit den Desktop-Status vertraut. Siehe „Desktop-Status virtueller Maschinen“, auf Seite 258.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Dashboard]** .

2 Erweitern Sie im Fenster **[Desktop Status (Desktop-Status)]** einen Statusordner.

Option	Beschreibung
Preparing (In Vorbereitung)	Listet die Desktop-Status auf, während die virtuelle Maschine bereitgestellt oder gelöscht wird bzw. sich im Wartungsmodus befindet.
Problem Desktops (Problematische Desktops)	Listet die Desktop-Fehlerstatus auf.
Prepared for use (Für die Verwendung vorbereitet)	Listet die Desktop-Status auf, wenn der Desktop verwendet werden kann.

3 Ermitteln Sie den Desktop-Status und klicken Sie auf die neben dem Status angezeigte Hyperlink-Nummer.

Auf der Seite **[Desktops]** werden alle Desktops mit dem ausgewählten Status angezeigt.

Weiter

Klicken Sie auf einen Desktop-Namen, um Einzelheiten zu diesem Desktop anzuzeigen, oder klicken Sie in View Administrator auf **[Back (Zurück)]**, um erneut auf die Dashboard-Seite zu wechseln.

Grundlegendes zu den View Manager-Diensten

Der Betrieb von View Connection Server-Instanzen und Sicherheitsservern hängt von verschiedenen Diensten ab, die auf dem System ausgeführt werden. Diese Systeme werden automatisch gestartet und beendet, aber gelegentlich kann es erforderlich sein, den Betrieb dieser Dienste manuell anzupassen.

Sie verwenden das Microsoft Windows-Tool **[Services (Dienste)]** zum Beenden oder Starten von View Manager-Diensten. Wenn Sie die View Manager-Dienste auf einem View Connection Server-Host oder einem Sicherheitsserver beenden, können die Endbenutzer sich erst wieder an ihren Desktops anmelden, wenn Sie die Dienste neu starten. Ein Neustart eines Dienstes kann erforderlich sein, wenn der Dienst nicht mehr ausgeführt wird oder die View Manager-Funktionalität eingeschränkt ist.

Beenden und Starten der View-Dienste

Der Betrieb von View Connection Server-Instanzen und Sicherheitsservern hängt von verschiedenen Diensten ab, die auf dem System ausgeführt werden. Gelegentlich kann es erforderlich sein, diese Dienste manuell zu beenden und zu starten, beispielsweise bei der Behebung von Problemen beim Betrieb von VMware View.

Wenn Sie View-Dienste beenden, können Endbenutzer sich nicht mehr an ihren Desktops anmelden. Sie sollten einen solchen Vorgang daher im Rahmen einer geplanten Systemwartung durchführen oder die Endbenutzer warnen, dass ihre Desktops temporär nicht zur Verfügung stehen werden.

HINWEIS Beenden Sie nur den VMware View Connection Server-Dienst auf einem View Connection Server-Host oder den VMware View Security Server-Dienst auf einem Sicherheitsserver. Beenden Sie keine anderen Komponentendienste.

Voraussetzungen

Machen Sie sich mit den Diensten vertraut, die auf View Connection Server-Hosts und Sicherheitsservern ausgeführt werden, wie beschrieben unter „Dienste auf einem View Connection Server-Host“, auf Seite 351 und „Dienste auf einem Sicherheitsserver“, auf Seite 351.

Vorgehensweise

1 Starten Sie das Windows-Tool **`Services (Dienste)`**, indem Sie an der Eingabeaufforderung **`services.msc`** eingeben.

2 Wählen Sie den VMware View Connection Server-Dienst auf einem View Connection Server-Host oder den VMware View Security Server-Dienst auf einem Sicherheitsserver und klicken Sie je nach gewünschtem Vorgang auf **[Stop (Beenden)]**, **[Restart (Neu starten)]** oder **[Start (Starten)]**.

3 Stellen Sie sicher, dass sich der Status des aufgeführten Dienstes wie erwartet ändert.

Dienste auf einem View Connection Server-Host

Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem View Connection Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

Tabelle 15-3. View Connection Server-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware View Connection Server	Automatisch	Stellt Verbindungs-Broker-Dienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework-, Nachrichtenbus-, Sicherheits-Gateway- und Webdienste gestartet oder beendet. Dieser Dienst führt keinen Start des VMware VDMDS-Dienstes oder des VMware View-Skripthostdienstes durch bzw. beendet diese Dienste nicht.
VMware View-Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.
VMware View-Nachrichtenbuskomponente	Manuell	Stellt Dienste für die Nachrichtenübermittlung zwischen View Manager-Komponenten bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.
VMware View, PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu View Connection Server über ein PCoIP Secure Gateway herstellen.
VMware View-Skripthost	Automatisch (falls aktiviert)	Bietet Unterstützung für Drittanbieterskripts, die beim Löschen von virtuellen Maschinen ausgeführt werden. Dieser Dienst ist standardmäßig deaktiviert. Sie sollten diesen Dienst aktivieren, wenn Sie Skripts ausführen möchten.
VMware View-Sicherheits-Gateway-Komponente	Manuell	Stellt sichere Tunneldienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.
VMware View-Webkomponente	Manuell	Stellt Webdienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden.
VMwareVDMDS	Automatisch	Stellt LDAP-Verzeichnisdienste für View Manager bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion von View Manager ausgeführt werden. Dieser Dienst muss auch bei Upgrades von VMware View ausgeführt werden, um die ordnungsgemäße Migration vorhandener Daten zu gewährleisten.

Dienste auf einem Sicherheitsserver

Der Betrieb von View Manager hängt von verschiedenen Diensten ab, die auf einem Sicherheitsserver ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

Tabelle 15-4. Dienste auf einem Sicherheitsserver

Dienstname	Starttyp	Beschreibung
VMware View Security Server	Automatisch	Stellt Sicherheitsserverdienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden. Wenn Sie diesen Dienst starten oder beenden, werden auch die Framework- und Sicherheits-Gateway-Dienste gestartet oder beendet.
VMware View-Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.

Tabelle 15-4. Dienste auf einem Sicherheitsserver (Fortsetzung)

Dienstname	Starttyp	Beschreibung
VMware View, PCoIP Secure Gateway	Manuell	Stellt Dienste für ein PCoIP Secure Gateway bereit. Dieser Dienst muss ausgeführt werden, wenn die Clients die Verbindung zu einem Sicherheitsserver über ein PCoIP Secure Gateway herstellen.
VMware View-Sicherheits-Gateway-Komponente	Manuell	Stellt sichere Tunneldienste bereit. Dieser Dienst muss zur ordnungsgemäßen Funktion eines Sicherheitsservers ausgeführt werden.

Dienste auf einem View Transfer Server-Host

Die Übertragungsvorgänge für lokale Desktops hängen von Diensten ab, die auf einem View Transfer Server-Host ausgeführt werden. Wenn Sie den Betrieb dieser Dienste anpassen möchten, müssen Sie sich zunächst mit ihnen vertraut machen.

Sämtliche der Dienste, die mit View Transfer Server installiert werden, müssen ausgeführt werden, um den ordnungsgemäßen Betrieb lokaler Desktops in View Manager zu gewährleisten.

Tabelle 15-5. View Transfer Server-Hostdienste

Dienstname	Starttyp	Beschreibung
VMware View Transfer Server	Automatisch	Stellt Dienste zur Koordination der View Transfer Server-bezogenen Dienste bereit. Wenn Sie diesen Dienst starten oder beenden, werden auch der View Transfer Server-Steuerungsdienst und der Framework-Dienst gestartet oder beendet.
VMware View Transfer Server-Steuerungsdienst	Manuell	Stellt Verwaltungsfunktionen für View Transfer Server bereit und sorgt für die Kommunikation mit View Connection Server.
VMware View-Framework-Komponente	Manuell	Stellt Dienste für Ereignisprotokollierung, Sicherheit und COM+-Framework für View Manager bereit.
Apache2.2-Dienst	Automatisch	Stellt Datenübertragungsfunktionen für Clientcomputer bereit, die View-Desktops im lokalen Modus ausführen. Der Apache2.2-Dienst wird gestartet, wenn Sie View Transfer Server zu View Manager hinzufügen.

Hinzufügen von Lizenzen zu VMware View

Wenn die aktuellen Lizenzen auf einem System ablaufen oder Sie auf VMware View-Funktionen zugreifen möchten, die derzeit nicht lizenziert sind, können Sie mithilfe von View Administrator Lizenzen hinzufügen.

Sie können eine Lizenz zu VMware View hinzufügen, während View Manager ausgeführt wird. Ein Neustart des Systems ist nicht erforderlich, und der Zugriff auf die Desktops wird nicht unterbrochen.

Voraussetzungen

Für den erfolgreichen Einsatz von View Manager und Add-On-Funktionen, wie beispielsweise View Composer und lokalen Desktops, müssen Sie einen gültigen Lizenzschlüssel erwerben.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (View-Konfiguration)] > [Product licensing and usage (Produktlizenzierung und -verwendung)]** und klicken Sie auf **[Edit license (Lizenz bearbeiten)]** .

2 Geben Sie die Seriennummer der Lizenz ein und klicken Sie auf **[OK]** .

Das Fenster **[Product Licensing (Produktlizenzierung)]** zeigt die aktualisierten Lizenzinformationen an.

Aktualisieren allgemeiner Benutzerinformationen aus Active Directory

Sie können View Manager mit den aktuellen Benutzerinformationen aktualisieren, die in Active Directory gespeichert sind. Diese Funktion aktualisiert Name, Telefonnummer, E-Mail-Adresse, Benutzername und die standardmäßige Windows-Domäne der View-Benutzer. Die vertrauenswürdigen externen Domänen werden ebenfalls aktualisiert.

Verwenden Sie diese Funktion, wenn Sie die Liste der vertrauenswürdigen externen Domänen in Active Directory ändern, insbesondere dann, wenn die geänderten Vertrauensbeziehungen zwischen Domänen sich auf Benutzerberechtigungen in View Manager auswirken.

Diese Funktion überprüft Active Directory auf die neuesten Benutzerinformationen und aktualisiert die View Manager-Konfiguration.

Sie können Benutzer- und Domäneninformationen auch über den Befehl `vdmadmin` aktualisieren. Siehe „Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F"", auf Seite 388.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[Users and Groups (Benutzer und Gruppen)]** .

2 Geben Sie an, ob die Informationen für alle Benutzer oder einen einzelnen Benutzer aktualisiert werden sollen.

Option	Aktion
Für alle Benutzer	Klicken Sie auf **[Update General User Information (Allgemeine Benutzerinformationen aktualisieren)]** . Das Aktualisieren aller Benutzer und Gruppen kann sehr viel Zeit beanspruchen.
Für einen einzelnen Benutzer	a Klicken Sie auf den Namen des Benutzers, für den Sie eine Aktualisierung durchführen möchten. b Klicken Sie auf **[Update General User Information (Allgemeine Benutzerinformationen aktualisieren)]** .

Migrieren von View Composer mit einer vorhandenen Datenbank

In bestimmten Situationen kann es erforderlich sein, einen View Composer-Dienst auf einen neuen Computer zu migrieren. Sie können hierbei die vorhandene View Composer-Datenbank weiterhin verwenden.

Sie können beispielsweise eine vCenter Server-Instanz auf einen neuen ESX-Host oder -Cluster migrieren, um Ihre Bereitstellung zu erweitern oder um die Instanz nach einem Hardwareausfall wiederherzustellen. Zur Beibehaltung Ihrer Linked-Clone-Desktops müssen Sie auch den mit vCenter Server installierten View Composer-Dienst migrieren.

Um den View Composer-Dienst zu migrieren, deinstallieren Sie den Dienst auf dem alten Computer und installieren ihn auf dem neuen Computer. Installationsanweisungen finden Sie im Dokument *Installation von VMware View*.

Die vorhandene View Composer-Datenbank muss auf einem verfügbaren Computer in derselben Domäne wie der Computer konfiguriert werden, auf dem Sie den neuen View Composer-Dienst installieren. Alternativ kann die Datenbank in einer vertrauenswürdigen Domäne konfiguriert werden.

View Composer erstellt RSA-Schlüsselpaare zum Ver- und Entschlüsseln der in der View Composer-Datenbank gespeicherten Authentifizierungsinformationen. Damit diese Datenquelle mit der neuen Instanz des View Composer-Dienstes kompatibel ist, müssen Sie zunächst den vom ursprünglichen View Composer-Dienst erstellten RSA-Schlüsselcontainer migrieren. Importieren Sie hierzu den RSA-Schlüsselcontainer auf den Computer, auf dem Sie den neuen Dienst installieren.

Hinweis Jede Instanz des View Composer-Dienstes muss über eine eigene View Composer-Datenbank verfügen. Mehrere View Composer-Dienste können eine View Composer-Datenbank nicht gemeinsam nutzen.

Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie die RSA-Schlüsselcontainer zwischen den Computern migrieren. Sie migrieren den RSA-Schlüsselcontainer mit dem Tool für die ASP.NET IIS-Registrierung, das zum Lieferumfang von Microsoft .NET Framework gehört.

Voraussetzungen

Sie können das .NET Framework unter den folgenden Webadressen herunterladen. Auf diesen Seiten erhalten Sie auch zusätzliche Informationen zum ASP .NET IIS-Registrierungstool:

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

Vorgehensweise

1 Installieren Sie das .NET Framework auf dem Computer, auf dem der mit der vorhandenen Datenbank verknüpfte View Composer-Dienst installiert ist.

2 Installieren Sie das .NET Framework auf dem Zielcomputer, auf dem Sie den neuen View Composer-Dienst installieren möchten.

Weiter

Migrieren Sie den RSA-Schlüsselcontainer auf den Zielcomputer. Siehe „Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst“, auf Seite 354.

Migrieren des RSA-Schlüsselcontainers auf den neuen View Composer-Dienst

Zur Verwendung einer vorhandenen View Composer-Datenbank müssen Sie die RSA-Schlüsselcontainer vom Quellcomputer, auf dem der vorhandene View Composer-Dienst installiert ist, auf den vCenter Server-Computer migrieren, auf dem Sie den neuen View Composer-Dienst installieren möchten.

Sie müssen diese Schritte ausführen, bevor Sie den neuen View Composer-Dienst installieren.

Voraussetzungen

Stellen Sie sicher, dass das Microsoft .NET Framework und das Tool für die ASP.NET IIS-Registrierung auf den Quell- und Zielcomputern installiert ist. Siehe „Vorbereiten eines Microsoft .NET Framework für das Migrieren von RSA-Schlüsseln“, auf Seite 354.

Vorgehensweise

1 Öffnen Sie auf dem Quellcomputer mit dem vorhandenen View Composer-Dienst eine Eingabeaufforderung und navigieren Sie zum Verzeichnis `%windir%\Microsoft.NET\Framework\v2.0`*xxxxx*.

2 Geben Sie den Befehl `aspnet_regiis` ein, um das RSA-Schlüsselpaar in einer lokalen Datei zu speichern.

```
aspnet_regiis –px "SviKeyContainer" "keys.xml" –pri
```

Das Tool für die ASP.NET IIS-Registrierung exportiert das RSA-Schlüsselpaar aus privatem und öffentlichem Schlüssel vom Container `SviKeyContainer` in die Datei `keys.xml` und speichert die Datei lokal.

3 Kopieren Sie die Datei `keys.xml` auf den Zielcomputer, auf dem Sie die neue Instanz des View Composer-Dienstes installieren möchten.

4 Öffnen Sie auf dem Zielcomputer eine Eingabeaufforderung und navigieren Sie zum Verzeichnis `%windir%\Microsoft.NET\Framework\v2.0`*xxxxx*.

5 Geben Sie den Befehl `aspnet_regiis` ein, um die RSA-Schlüsselpaardaten zu migrieren.

```
aspnet_regiis –pi "SviKeyContainer" "Pfad\keys.xml"
```

Hierbei steht *Pfad* für den Pfad zur exportierten Datei.

Das Registrierungstool importiert das Schlüsselpaar in den lokalen Schlüsselcontainer.

Weiter

Installieren Sie den neuen View Composer-Dienst auf dem vCenter Server-Zielcomputer. Installationsanweisungen finden Sie im Dokument *Installation von VMware View*.

Aktualisieren der Zertifikate auf einer View Connection Server-Instanz oder einem Sicherheitsserver

Wenn Sie aktualisierte SSL-Zertifikate oder Zwischenzertifikate erhalten, importieren Sie die Zertifikate in eine neue Schlüsselspeicherdatei und konfigurieren die Datei `locked.properties` auf jedem View Connection Server- oder Sicherheitsserverhost zur Verwendung der neuen Schlüsselspeicherdatei.

Üblicherweise verlieren Serverzertifikate nach 12 Monaten ihre Gültigkeit. Stamm- und Zwischenzertifikate laufen nach 5 oder 10 Jahren ab.

Wenn Sie Zertifikate in eine Schlüsselspeicherdatei importieren, wird der Schlüsselspeicher über den Befehl `keytool` erstellt, sofern die angegebene Datei nicht vorhanden ist.

Die neue Schlüsselspeicherdatei muss einen anderen Namen aufweisen als die vorhandene Schlüsselspeicherdatei. VMware empfiehlt, das Ablaufdatum in den Dateinamen aufzunehmen. Beispiel: `keys_2014123.jks`.

Sie müssen eine Java-Schlüsselspeicherdatei angeben, wenn Sie Zwischenzertifikate importieren. Wenn Sie keine Zwischenzertifikate verwenden, können Sie anstelle einer Java-Schlüsselspeicherdatei (`jks`) eine PKCS#12- oder PFX-Datei angeben.

Weitere Informationen zum Erstellen einer Schlüsselspeicherdatei und zum Importieren von Server- und Zwischenzertifikaten in die Schlüsselspeicherdatei finden Sie im Dokument *Installation von VMware View*.

Voraussetzungen

Fordern Sie aktualisierte Server- und Zwischenzertifikate von der Zertifizierungsstelle an, bevor die aktuellen Zertifikate ablaufen.

Vorgehensweise

1 Wenn Sie Zwischenzertifikate verwenden, importieren Sie die aktualisierten Zwischenzertifikate in eine neue Schlüsselspeicherdatei im selben Verzeichnis wie die vorhandene Schlüsselspeicherdatei.

Beispiel:

```
keytool –importcert –keystore keys_20141231.jks –storepass secret –trustcacerts –alias intermediateCA –file intermediateCA.cer
```

2 Importieren Sie die aktualisierten Serverzertifikate in die neue Schlüsselspeicherdatei.

Beispiel:
keytool –importcert –keystore keys_20141231.jks –storepass secret –keyalg "RSA" –trustcacerts –file certificate.p7

3 Bearbeiten Sie die Eigenschaften `keyfile` und `keypass` in der Datei `locked.properties` auf dem View Connection Server- oder Sicherheitsserverhost.

a Legen Sie die Eigenschaft `keyfile` auf den Namen der neuen Schlüsselspeicherdatei fest.

Beispiel:

```
keyfile=keys_20141231.jks
```

b Wenn das Kennwort für die Schlüsselspeicherdatei geändert wurde, legen Sie die Eigenschaft `keypass` auf das neue Kennwort fest.

Beispiel:

```
keypass=NEUES_KENNWORT
```

4 Stellen Sie sicher, dass die Eigenschaft `storetype` in der Datei `locked.properties` mit dem Typ der Schlüsselspeicherdatei übereinstimmt.

Option	Beschreibung
PKCS#12- oder PFX-Datei	Legen Sie für `storetype` den Wert **`pkcs12`** fest.
Java-Schlüsselspeicherdatei	Legen Sie für `storetype` den Wert **`jks`** fest.

Beispiel:

```
storetype=jks
```

Für eine Java-Schlüsselspeicherdatei muss die Eigenschaft `storetype` angegeben werden.

5 Starten Sie den View Connection Server- oder Sicherheitsserverdienst neu, damit die Änderungen wirksam werden.

Fehlerbehebung bei View-Komponenten 16

Zur Diagnose und Behandlung von Problemen, die bei Verwendung von View Manager, View Composer und View Client auftreten können, sind verschiedene Vorgehensweisen verfügbar.

Für Administratoren kann es bei Verwendung von View Manager und View Composer zu einem unerwarteten Verhalten kommen, das behandelt werden muss. Für die Benutzer kann es bei Verwendung von View Client für den Zugriff auf ihre Desktops zu Problemen kommen. Sie können die Vorgehensweisen zur Fehlerbehebung nutzen, um die Ursachen dieser Probleme zu ermitteln. Anschließend können Sie versuchen, die Probleme selbst zu behandeln, oder sich an den technischen Support von VMware wenden, um Unterstützung zu erhalten.

Dieses Kapitel behandelt die folgenden Themen:

- „Überwachen des Systemzustands“, auf Seite 358
- „Überwachen von Ereignissen in View Manager“, auf Seite 358
- „Senden von Nachrichten an Desktop-Benutzer“, auf Seite 359
- „Anzeigen von Desktops, auf denen Probleme vermutet werden“, auf Seite 359
- „Verwalten von Desktops und Richtlinien für nicht berechtigte Benutzer“, auf Seite 360
- „Sammeln von Diagnoseinformationen für VMware View“, auf Seite 361
- „Aktualisieren von Supportanfragen“, auf Seite 365
- „Weitere Informationen zur Fehlerbehebung“, auf Seite 365
- „Fehlerbehebung bei Problemen mit der Netzwerkverbindung“, auf Seite 365
- „Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung“, auf Seite 370
- „Fehlerbehebung bei Problemen mit der USB-Umleitung“, auf Seite 373
- „Beheben von Fehlern bei der QuickPrep-Anpassung“, auf Seite 375
- „View Composer-Bereitstellungsfehler“, auf Seite 376
- „Fehler beim Hinzufügen von verknüpften Windows XP-Klonen zur Domäne“, auf Seite 378
- „Fehlerbehebung von GINA-Problemen auf Windows XP-Desktops“, auf Seite 378

Überwachen des Systemzustands

Mithilfe des Dashboards zum Systemzustand in View Administrator können Sie rasch Probleme ermitteln, die sich auf die Ausführung von View oder den Benutzerzugriff auf Desktops auswirken können.

Das Dashboard zum Systemzustand befindet sich oben links in der View Administrator-Anzeige und bietet verschiedene Links, um Berichte zur Ausführung von View Manager anzuzeigen:

Remote Sessions (Remote-Sitzungen)	Bietet einen Link zum Bildschirm **[Global Remote Sessions (Globale Remote-Sitzungen)]** , in dem Informationen zum Status von Remote-Sitzungen angezeigt werden.
Local Sessions (Lokale Sitzungen)	Bietet einen Link zum Bildschirm **[Global Local Sessions View (Globale Ansicht lokaler Sitzungen)]** , in dem Informationen zum Status lokaler Desktop-Sitzungen angezeigt werden.
Problem Desktops (Problematische Desktops)	Bietet einen Link zum Bildschirm **[Global Desktop View (Globale Desktop-Ansicht)]** , in dem Informationen zu Desktops angezeigt werden, die von View Manager als problematisch gekennzeichnet wurden.
Events (Ereignisse)	Bietet Links zum Bildschirm **[Events (Ereignisse)]** , der nach Ereignissen und Warnungsereignissen gefiltert ist.
System Health (Systemzustand)	Bietet Links zum Bildschirm **[Dashboard]** , in dem der Status von View-Komponenten, vSphere-Komponenten, Domänen, Desktops und Informationen zur Datenspeichernutzung zusammengefasst werden.

Das Dashboard zum Systemzustand zeigt für jedes Element einen nummerierten Link an. Dieser Wert gibt die Anzahl an Elementen an, zu denen der verknüpfte Bericht Details enthält.

Überwachen von Ereignissen in View Manager

In der Ereignisdatenbank werden Informationen zu Ereignissen gespeichert, die im View Connection Server-Host oder in der View Connection Server-Gruppe, in den View Agent-Instanzen und in View Administrator auftreten. Sie werden im Dashboard über die Anzahl an Ereignissen benachrichtigt. Im Ereignisbildschirm können Sie die Ereignisse im Detail untersuchen.

Hinweis Ereignisse werden in der View Administrator-Oberfläche für einen begrenzten Zeitraum angezeigt. Nach Ablauf dieses Zeitraums stehen die Ereignisse nur in den Verlaufsdatenbanktabellen zur Verfügung. Sie können die Ereignisse in den Datenbanktabellen unter Verwendung von Microsoft SQL Server oder Oracle-Datenbankberichttools untersuchen. Weitere Informationen finden Sie im Dokument *Integration von VMware View*.

Voraussetzungen

Erstellen und konfigurieren Sie die Ereignisdatenbank. Die erforderlichen Schritte sind im Dokument *Installation von VMware View* beschrieben.

Vorgehensweise

1 Wählen Sie in View Administrator **[Monitoring (Überwachung)] > [Events (Ereignisse)]** .

2 (Optional) Im Ereignisfenster können Sie den Zeitraum der Ereignisse auswählen, die Ereignisse filtern und die aufgelisteten Ereignisse nach einer oder mehreren Spalten sortieren.

View Manager-Ereignismeldungen

View Manager zeigt ein Ereignis an, wenn sich der Systemstatus ändert oder ein Problem ermittelt wird. Basierend auf den in den Ereignismeldungen enthaltenen Informationen können Sie die entsprechende Maßnahme ergreifen.

Tabelle 16-1 zeigt die Ereignistypen, die in View Manager angezeigt werden.

Tabelle 16-1. Von View Manager angezeigte Ereignistypen

Ereignistyp	Beschreibung
Audit Failure or Audit Success (Überwachungsfehler oder Überwachungserfolg)	Zeigt das Fehlschlagen oder den Erfolg einer Änderung an, die ein Administrator oder Benutzer am Verhalten oder an der Konfiguration von VMware View vornimmt.
Error (Fehler)	Zeigt einen fehlgeschlagenen View Manager-Vorgang an.
Information	Zeigt normale Vorgänge innerhalb von VMware View an.
Warning (Warnung)	Zeigt kleinere Probleme bei Vorgängen oder Konfigurationseinstellungen an, die zu schwerwiegenderen Problemen führen könnten.

Für Überwachungsfehler, Fehler oder Warnungen müssen möglicherweise Maßnahmen ergriffen werden. Wenn Überwachungserfolge oder Informationen angezeigt werden, sind keine Schritte erforderlich.

Senden von Nachrichten an Desktop-Benutzer

In einigen Fällen kann es erforderlich sein, Nachrichten an Benutzer zu senden, die gegenwärtig an Desktops angemeldet sind. Wenn Sie beispielsweise Wartungsaufgaben für einen Desktop ausführen müssen, können Sie den Benutzer bitten, sich vorübergehend abzumelden. Oder Sie senden eine Warnung zu zukünftigen Dienstunterbrechungen an die Benutzer.

Vorgehensweise

1. Wählen Sie in View Administrator **[Users and Groups (Benutzer und Gruppen)]** .
2. Klicken Sie auf den Benutzer, an den Sie eine Nachricht senden möchten.
3. Wählen Sie auf der Registerkarte **[Sessions (Sitzungen)]** die Sitzung des Benutzers und klicken Sie auf **[Send Message (Nachricht senden)]** .
4. Geben Sie den Nachrichtentext ein, wählen Sie den Nachrichtentyp aus und klicken Sie auf **[OK]** .

Anzeigen von Desktops, auf denen Probleme vermutet werden

Sie können eine Liste der von View Manager ermittelten Desktops anzeigen, auf denen Probleme vermutet werden.

View Administrator zeigt Desktops mit den folgenden Problemen an:

- Eingeschaltete Desktops, die nicht reagieren.
- Desktops, die während eines langen Zeitraums den Bereitstellungsstatus aufweisen.
- Desktops, die bereit sind, jedoch keine Verbindungen akzeptieren.
- Desktops, die auf einer vCenter Server-Instanz fehlen.
- Desktops, die über aktive Konsolenanmeldungen, Anmeldungen durch nicht berechtigte Benutzer oder Anmeldungen über eine View Connection Server-Instanz verfügen.

Vorgehensweise

1 Wählen Sie in View Administrator **[Desktops]** .

2 Klicken Sie auf der Registerkarte **[VirtualCenter VMs (VirtualCenter-VMs)]** auf **[Problem Desktops (Problematische Desktops)]** .

Weiter

Die erforderliche Maßnahme hängt davon ab, welches Problem View Administrator für einen Desktop meldet.

- Wenn ein Desktop eingeschaltet ist, jedoch nicht reagiert, starten Sie die virtuelle Maschine neu. Reagiert der Desktop weiterhin nicht, stellen Sie sicher, dass das Desktop-Betriebssystem die View Agent-Version unterstützt. Siehe „Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A"", auf Seite 385.
- Wenn ein Desktop während eines langen Zeitraums den Bereitstellungsstatus aufweist, löschen Sie die virtuelle Maschine und führen den Klonvorgang für diese Maschine erneut aus. Stellen Sie sicher, dass ausreichend Festplattenspeicherplatz für die Bereitstellung des Desktops verfügbar ist. Siehe „Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen", auf Seite 373.
- Wenn ein Desktop bereit ist, jedoch keine Verbindungen akzeptiert, überprüfen Sie die Firewall-Konfiguration, um sicherzustellen, dass das Anzeigeprotokoll (RDP oder PCoIP) nicht blockiert wird. Siehe „Verbindungsprobleme zwischen Desktops und View Connection Server-Instanzen", auf Seite 368.
- Wenn ein Desktop auf einer vCenter Server-Instanz nicht angezeigt wird, überprüfen Sie, ob die virtuelle Maschine auf der erwarteten vCenter Server-Instanz konfiguriert ist oder auf eine andere vCenter Server-Instanz verschoben wurde.
- Wenn ein Desktop über eine aktive Anmeldung verfügt, dies jedoch keine Konsolenanmeldung ist, muss es sich um eine Remote-Sitzung handeln. Wenn die angemeldeten Benutzer nicht kontaktiert werden können, muss die virtuelle Maschine möglicherweise neu gestartet werden, um die Abmeldung der Benutzer zu erzwingen.

Verwalten von Desktops und Richtlinien für nicht berechtigte Benutzer

Sie können die Desktops von Benutzern anzeigen, deren Berechtigungen entfernt wurden. Zudem können Sie die Richtlinien anzeigen, die auf nicht berechtigte Benutzer angewendet werden.

Ein Benutzer ohne Berechtigung hat möglicherweise die Organisation verlassen oder das Konto wurde für einen längeren Zeitraum gesperrt. Diese Benutzer verfügen über einen zugewiesenen Desktop, sind jedoch nicht länger zur Verwendung des Desktop-Pools berechtigt.

Über den Befehl `vdmadmin` können Sie nicht berechtigte Desktops und Richtlinien anzeigen. Siehe „Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O" und „-P"", auf Seite 400.

Vorgehensweise

1 Wählen Sie in View Administrator **[Desktops]** .

2 Wählen Sie **[More Commands (Weitere Befehle)] > [View Unentitled Machines (Maschinen nicht berechtigter Benutzer anzeigen)]** .

3 Entfernen Sie die Desktop-Zuweisungen für nicht berechtigte Benutzer und führen Sie ein Rollback lokaler Desktops durch, die von nicht berechtigten Benutzern ausgecheckt wurden.

4 Wählen Sie **[More Commands (Weitere Befehle)] > [View Unentitled Machines (Maschinen nicht berechtigter Benutzer anzeigen)]** oder **[More Commands (Weitere Befehle)] > [View Unentitled Policies (Richtlinien nicht berechtigter Benutzer anzeigen)]** .

5 Ändern oder entfernen Sie die Richtlinien, die auf nicht berechtigte Benutzer angewendet werden.

Sammeln von Diagnoseinformationen für VMware View

Sie können Diagnoseinformationen sammeln, um den technischen Support von VMware bei der Diagnose und Behandlung von Problemen mit VMware View zu unterstützen.

Sie können Diagnoseinformationen für verschiedene Komponenten von VMware View sammeln. Wie diese Informationen gesammelt werden, variiert abhängig von der VMware View-Komponente.

- Erstellen eines Data Collection Tool-Pakets für View Agent auf Seite 361

  Um den technischen Support von VMware bei der Fehlerbehebung für View Agent zu unterstützen, müssen Sie möglicherweise den Befehl `vdmadmin` zum Erstellen eines DCT-Pakets (Data Collection Tool) verwenden.

- Speichern von Diagnoseinformationen für View Client auf Seite 362

  Wenn bei Verwendung von View Client Probleme auftreten, die sich mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen nicht lösen lassen, können Sie eine Kopie der Protokolldateien und Informationen zur Konfiguration speichern.

- Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts auf Seite 362

  Mithilfe des View Composer-Supportskripts können Sie Konfigurationsdaten sammeln und Protokolldateien für View Composer generieren. Diese Informationen erleichtern den Mitarbeitern des Kundensupports von VMware die Diagnose von Problemen im Zusammenhang mit View Composer.

- Sammeln von Diagnoseinformationen für View Connection Server mithilfe des Supporttools auf Seite 363

  Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für View Connection Server generieren.

- Sammeln von Diagnoseinformationen für View Agent, View Client oder View Connection Server von der Konsole auf Seite 364

  Wenn Sie über direkten Zugriff auf die Konsole verfügen, können Sie die Supportskripts zur Generierung von Protokolldateien für View Connection Server, View Client oder für Desktops verwenden, auf denen View Agent ausgeführt wird. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit diesen Komponenten.

Erstellen eines Data Collection Tool-Pakets für View Agent

Um den technischen Support von VMware bei der Fehlerbehebung für View Agent zu unterstützen, müssen Sie möglicherweise den Befehl `vdmadmin` zum Erstellen eines DCT-Pakets (Data Collection Tool) verwenden.

Sie müssen an einer Standard- oder Replikatinstanz von View Connection Server mit der Rolle **Administrators (Administratoren)** angemeldet sein.

Vorgehensweise

- Um den Namen der Ausgabepaketdatei, des Desktop-Pools und der Maschine anzugeben, verwenden Sie die Optionen `–outfile`, `–d` und `–m` mit dem Befehl `vdmadmin`.

  ```
  vdmadmin –A [–b Authentifizierungsargumente] –getDCT –outfile lokale_Datei –d Desktop –m Maschine
  ```

Der Befehl schreibt das Paket in die angegebene Ausgabedatei.

Beispiel: Erstellen einer Paketdatei für View Agent

Erstellen Sie das DCT-Paket für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** und schreiben Sie es in die .zip-Datei `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Weiter

Wenn bereits eine Supportanfrage geöffnet wurde, können Sie sie aktualisieren, indem Sie die DCT-Paketdatei anfügen.

Speichern von Diagnoseinformationen für View Client

Wenn bei Verwendung von View Client Probleme auftreten, die sich mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen nicht lösen lassen, können Sie eine Kopie der Protokolldateien und Informationen zur Konfiguration speichern.

Sie können versuchen, Verbindungsprobleme mit View Client zu lösen, bevor Sie die Diagnoseinformationen speichern und sich an den technischen Support von VMware wenden. Weitere Informationen finden Sie unter „Verbindungsprobleme zwischen View Client und View Connection Server“, auf Seite 365.

Vorgehensweise

1 Klicken Sie in View Client auf **[Support Information (Support-Informationen)]** oder wählen Sie im Menü für den virtuellen Desktop **[Options (Optionen)] > [Support Information (Support-Informationen)]** .

2 Klicken Sie im Fenster **[Support Information (Support-Informationen)]** auf **[Collect Support Data (Supportdaten sammeln)]** und klicken Sie bei Aufforderung auf **[Yes (Ja)]** .

   Ein Befehlsfenster zeigt den Fortschritt beim Sammeln der Informationen. Dieser Vorgang kann einige Minuten dauern.

3 Geben Sie im Befehlsfenster bei Aufforderung die URLs der View Connection Server-Instanzen ein, für die Sie die Konfiguration von View Client testen möchten. Aktivieren Sie ggf. die Option zum Generieren von Diagnose-Dumps der VMware View-Prozesse.

   Die Informationen werden in eine ZIP-Datei in einen Ordner auf dem Desktop des Clientcomputers geschrieben.

4 Senden Sie über die Support-Seite der VMware-Website eine Support-Anfrage und fügen Sie die ZIP-Ausgabedatei an.

Sammeln von Diagnoseinformationen für View Composer mithilfe des Supportskripts

Mithilfe des View Composer-Supportskripts können Sie Konfigurationsdaten sammeln und Protokolldateien für View Composer generieren. Diese Informationen erleichtern den Mitarbeitern des Kundensupports von VMware die Diagnose von Problemen im Zusammenhang mit View Composer.

Voraussetzungen

Melden Sie sich an der vCenter Server-Instanz an, auf der View Composer installiert ist.

Da Sie zum Ausführen des Supportskripts das Windows Script Host-Dienstprogramm (`cscript`) verwenden müssen, machen Sie sich mit dem Befehl `cscript` vertraut. Siehe http://technet.microsoft.com/library/bb490887.aspx.

Vorgehensweise

1 Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis `C:\Programme\VMware\VMware View Composer`.

   Wenn Sie die Software nicht in den Standardverzeichnissen installiert haben, ersetzen Sie den entsprechenden Laufwerkbuchstaben und Pfad.

2 Geben Sie den Befehl zur Ausführung des `svi-support`-Skripts ein.

```
cscript ".\svi-support.wsf /zip"
```

Über die Option `/?` können Sie Informationen zu anderen Befehlsoptionen anzeigen, die mit dem Skript verwendet werden können.

Nach Ausführung des Skripts werden Sie über den Namen und Speicherort der Ausgabedatei informiert.

3 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedatei an.

Sammeln von Diagnoseinformationen für View Connection Server mithilfe des Supporttools

Mithilfe des Supporttools können Sie Protokollierungsebenen festlegen und Protokolldateien für View Connection Server generieren.

Das Supporttool sammelt Protokollierungsdaten für View Connection Server. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit View Connection Server. Das Supporttool ist nicht geeignet, um Diagnoseinformationen für View Client oder View Agent zu sammeln. Für diese Komponenten muss stattdessen das Supportskript verwendet werden. Siehe „Sammeln von Diagnoseinformationen für View Agent, View Client oder View Connection Server von der Konsole“, auf Seite 364.

Voraussetzungen

Melden Sie sich an einer Standard- oder Replikatinstanz von View Connection Server als Benutzer mit der Rolle **Administrators (Administratoren)** angemeldet sein.

Vorgehensweise

1 Wählen Sie **[Start] > [All Programs (Alle Programme)] > [VMware] > [Set View Connection Server Log Levels (View Connection Server-Protokollebene festlegen)]** .

2 Geben Sie im Textfeld **[Choice (Auswahl)]** einen numerischen Wert zur Festlegung der Protokollierungsebene ein und drücken Sie die Eingabetaste.

Option	Beschreibung
0	Setzt die Protokollierungsebene auf den Standardwert zurück.
1	Legt die normale Protokollierungsebene (Standardeinstellung) fest.
2	Legt die Debug-Protokollierungsebene fest.
3	Legt die vollständige Protokollierung fest.

Normalerweise sollten Sie den Wert **2** eingeben, um eine Debug-Protokollierungsebene zu wählen.

Das System beginnt unter Verwendung der ausgewählten Protokollierungsebene mit der Aufzeichnung von Protokollinformationen.

3 Wenn Sie genügend Informationen zum Verhalten von View Connection Server gesammelt haben, wählen Sie **[Start] > [All Programs (Alle Programme)] > [VMware] > [Generate View Connection Server Log Bundle (View Connection Server-Protokollsatz generieren)]** .

Das Supporttool schreibt die Protokolldateien in den Ordner `vdm-sdct` auf dem Desktop der View Connection Server-Instanz.

4 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedateien an.

Sammeln von Diagnoseinformationen für View Agent, View Client oder View Connection Server von der Konsole

Wenn Sie über direkten Zugriff auf die Konsole verfügen, können Sie die Supportskripts zur Generierung von Protokolldateien für View Connection Server, View Client oder für Desktops verwenden, auf denen View Agent ausgeführt wird. Diese Informationen erleichtern den Mitarbeitern des technischen Supports von VMware die Diagnose von Problemen im Zusammenhang mit diesen Komponenten.

Voraussetzungen

Melden Sie sich an dem System an, für das Sie Informationen sammeln möchten.

- Für View Agent melden Sie sich an der virtuellen Maschine an, auf der View Agent installiert ist.
- Für View Client melden Sie sich an dem System an, auf dem View Client installiert ist.
- Für View Connection Server melden Sie sich am View Connection Server-Host an.

Vorgehensweise

1 Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis der VMware View-Komponente, für die Diagnoseinformationen gesammelt werden sollen.

Option	Beschreibung
View Agent	Wechseln Sie in das Verzeichnis `C:\Programme\VMware View\Agent\DCT`.
View Client	Wechseln Sie in das Verzeichnis `C:\Programme\VMware View\Client\DCT`.
View Connection Server	Wechseln Sie in das Verzeichnis `C:\Programme\VMware View\Server\DCT`.

Wenn Sie die Software nicht in den Standardverzeichnissen installiert haben, ersetzen Sie den entsprechenden Laufwerkbuchstaben und Pfad.

2 Geben Sie den Befehl zur Ausführung des Supportskripts ein.

```
.\support.bat [loglevels]
```

Wenn Sie die erweiterte Protokollierung aktivieren möchten, verwenden Sie die Option `loglevels` und geben bei Aufforderung den numerischen Wert für die Protokollierungsebene ein.

Option	Beschreibung
0	Setzt die Protokollierungsebene auf den Standardwert zurück.
1	Legt die normale Protokollierungsebene (Standardeinstellung) fest.
2	Legt die Debug-Protokollierungsebene fest.
3	Legt die vollständige Protokollierung fest.
4	Legt die Protokollierung von Informationen für PCoIP fest (nur bei View Agent und View Client).
5	Legt die Debug-Protokollierung für PCoIP fest (nur bei View Agent und View Client).
6	Legt die Protokollierung von Informationen für virtuelle Kanäle fest (nur bei View Agent und View Client).
7	Legt die Debug-Protokollierung für virtuelle Kanäle fest (nur bei View Agent und View Client).
8	Legt die Ablaufprotokollierung für virtuelle Kanäle fest (nur bei View Agent und View Client).

Das Skript schreibt die komprimierten Protokolldateien in den Ordner `vdm-sdct` auf dem Desktop.

3 Die View Composer Guest Agent-Protokolle werden im Verzeichnis `C:\Programme\Gemeinsame Dateien\VMware\View Composer Guest Agent svi-ga-support` gespeichert.

4 Senden Sie über die Supportseite der VMware-Website eine Supportanfrage und fügen Sie die Ausgabedatei an.

Aktualisieren von Supportanfragen

Sie können eine vorhandene Supportanfrage auf der Support-Website aktualisieren.

Nachdem Sie eine Supportanfrage gesendet haben, erhalten Sie möglicherweise eine E-Mail vom technischen Support von VMware, in der Sie zur Bereitstellung der Ausgabedateien des Skripts `support` oder `svi-support` aufgefordert werden. Bei der Ausführung der Skripts werden Sie über den Namen und Speicherort der Ausgabedatei informiert. Antworten Sie auf diese E-Mail und hängen Sie die Ausgabedatei an Ihre Antwort an.

Wenn die Ausgabedatei für eine E-Mail-Anlage zu groß ist (10 MB oder mehr), wenden Sie sich unter Angabe der Supportanfragenummer an den technischen Support von VMware und bitten Sie um Anweisungen für einen FTP-Upload. Alternativ können Sie die Datei auf der Support-Website an Ihre vorhandene Supportanfrage anfügen.

Vorgehensweise

1 Wechseln Sie zur Supportseite der VMware-Website und melden Sie sich an.

2 Klicken Sie auf **[Support Request History (Supportanfrageverlauf)]** und suchen Sie nach der gewünschten Supportanfragenummer.

3 Aktualisieren Sie Ihre Supportanfrage und hängen Sie die Ausgabedatei des Skripts `support` oder `svi-support` an.

Weitere Informationen zur Fehlerbehebung

Weitere Informationen zur Fehlerbehebung finden Sie in VMware Knowledge Base-Artikeln.

Die VMware Knowledge Base (KB) wird kontinuierlich mit neuen Informationen zur Fehlerbehebung für VMware-Produkte aktualisiert.

Weitere Informationen zur Fehlerbehebung für View Manager finden Sie in den KB-Artikeln auf der VMware KB-Website:

http://kb.vmware.com/selfservice/microsites/microsite.do

Fehlerbehebung bei Problemen mit der Netzwerkverbindung

Für die Diagnose und Behandlung von Problemen mit der Netzwerkverbindung zu Desktops oder View Client- und View Connection Server-Instanzen können Sie zwischen verschiedenen Vorgehensweisen wählen.

Verbindungsprobleme zwischen View Client und View Connection Server

Bei der Verbindung zwischen View Client und View Connection Server können Probleme auftreten.

Problem

Wenn es bei der Konnektivität zwischen View Client und einer View Connection Server-Instanz zu einem Fehler kommt, wird für View Client einer der folgenden Fehler angezeigt:

- `A secure connection to the server '`*`servername`*`' cannot be established. (Es konnte keine sichere Verbindung mit dem Server '`*`Servername`*`' hergestellt werden.)`

- `The View Connection Server connection failed. (Die Verbindung zum View Connection Server ist fehlgeschlagen.)`

Auch das Öffnen eines Desktops kann fehlschlagen, nachdem eine View Connection Server-Instanz kontaktiert und eine Liste der verfügbaren Desktops abgerufen wurde.

Ursache

Bei der Konnektivität zwischen View Client und einer View Connection Server-Instanz können aus verschiedenen Gründen Probleme auftreten.

- Falsche Netzwerk-Proxy- oder Firewall-Einstellungen auf der View Client-Instanz.
- Lookup-Fehler für den DNS-Namen des View Connection Server-Hosts bei der Einrichtung einer sicheren Verbindung.

Lösung

Führen Sie zur Problemlösung nacheinander die folgenden Verfahren aus. Wenn ein Lösungsvorschlag nicht zur Beseitigung des Problems führt, führen Sie das nächste Verfahren aus.

- Greifen Sie über einen Browser unter Verwendung von HTTP oder HTTPS auf die View Connection Server-Instanz zu.

  Wenn die Anmeldeseite nicht angezeigt wird, behandeln Sie das Problem mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen.
- Geben Sie auf der Anmeldeseite gültige Anmeldeinformationen ein.
- Wenn in einer Fehlermeldung angezeigt wird, dass die sichere Verbindung nicht hergestellt werden kann, ist die Ursache wahrscheinlich, dass View Client (oder der Proxy-Server, sofern konfiguriert) den DNS-Namen des View Connection Server-Hosts nicht auflösen kann. Konfigurieren Sie den Host zur Bereitstellung der IP-Adresse anstelle des vollqualifizierten Domänennamens (FQDN), wenn View Client zum Öffnen einer sicheren Verbindung angewiesen wird.

  a Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration) > Servers (Server)]** .

  b Wählen Sie die gewünschte Sicherheitsserver- oder View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .

  c Stellen Sie sicher, dass im Textfeld für die externe PCoIP-URL die externe IP-Adresse für die Sicherheitsserver- oder View Connection Server-Instanz angegeben ist, anhand derer View Client-Instanzen über das Internet zugreifen können.

  d Klicken Sie auf **[OK]** .

  Die externe URL wird sofort aktualisiert. Der View Connection Server-Dienst muss nicht neu gestartet werden, damit die Änderung übernommen wird.
- Wenn das Problem durch die zuvor beschriebene Lösung nicht gelöst wird, starten Sie die View Connection Server-Instanz neu.

Verbindungsprobleme zwischen View Client und dem sicheren PCoIP-Gateway

Es kann zu Verbindungsproblemen zwischen View Client und einem Sicherheitsserver- oder View Connection Server-Host kommen, wenn das sichere PCoIP-Gateway so konfiguriert ist, dass externe Benutzer, die über PCoIP kommunizieren, authentifiziert werden müssen.

Problem

View Client-Instanzen, die PCoIP verwenden, können weder eine Verbindung mit View-Desktops herstellen noch diese anzeigen. Die anfängliche Anmeldung an einer Sicherheitsserver- oder View Connection Server-Instanz ist erfolgreich, die Verbindung schlägt jedoch fehl, wenn der Benutzer einen View-Desktop auswählt. Dieses Problem tritt auf, wenn das sichere PCoIP-Gateway auf einem Sicherheitsserver- oder View Connection Server-Host konfiguriert ist.

Hinweis Normalerweise wird das sichere PCoIP-Gateway auf einem Sicherheitsserver eingesetzt. In einer Netzwerkkonfiguration, bei der externe Clients eine direkte Verbindung mit dem View Connection Server-Host herstellen, kann das sichere PCoIP-Gateway auch auf der View Connection Server-Instanz konfiguriert werden.

Ursache

Es kann verschiedene Gründe dafür geben, dass Probleme bei der Verbindungsherstellung mit dem sicheren PCoIP-Gateway auftreten.

- In der Windows-Firewall wurde ein Port geschlossen, der für das sichere PCoIP-Gateway erforderlich ist.
- Das sichere PCoIP-Gateway ist auf der Sicherheitsserver- oder View Connection Server-Instanz nicht aktiviert.
- Die externe PCoIP-URL ist falsch konfiguriert. Sie müssen diese Einstellung auf die externe IP-Adresse festlegen, auf die View Client-Instanzen über das Internet zugreifen können.
- Die externe PCoIP-URL oder die externe URL des sicheren Tunnels ist so konfiguriert, dass sie auf einen anderen Sicherheitsserver oder View Connection Server-Host verweist. Wenn Sie diese beiden externen URLs auf einem Sicherheitsserver- oder View Connection Server-Host konfigurieren, muss es sich bei beiden externen URLs um Adressen für den aktuellen Host handeln.
- Die View Client-Instanz stellt die Verbindung über einen externen Webproxy her, für den ein Port geschlossen wurde, der für das sichere PCoIP-Gateway erforderlich ist. Beispielsweise kann ein Webproxy im Netzwerk eines Hotels oder eine öffentliche drahtlose Verbindung die erforderlichen Ports blockieren.
- Die View Connection Server-Instanz, die mit dem Sicherheitsserver kombiniert ist, auf dem das sichere PCoIP-Gateway konfiguriert ist, verwendet View 4.5 oder eine frühere Version. Der Sicherheitsserver und die kombinierte View Connection Server-Instanz müssen View 4.6 oder eine höhere Version verwenden.

Lösung

- Stellen Sie sicher, dass die folgenden Netzwerkports in der Firewall für den Sicherheitsserver- oder View Connection Server-Host geöffnet sind.

Port	Beschreibung
TCP 4172	Von der View Client-Instanz zum Sicherheitsserver- oder View Connection Server-Host.
UDP 4172	Zwischen der View Client-Instanz und dem Sicherheitsserver- oder View Connection Server-Host, in beide Richtungen.
TCP 4172	Vom Sicherheitsserver- oder View Connection Server-Host zum View-Desktop.
UDP 4172	Zwischen dem Sicherheitsserver- oder View Connection Server-Host und dem View-Desktop, in beide Richtungen.

- Aktivieren Sie in View Administrator das sichere PCoIP-Gateway und stellen Sie sicher, dass die externe PCoIP-URL richtig konfiguriert ist.
  a Klicken Sie auf **[View Configuration (View-Konfiguration)] > [Server]** .
  b Wählen Sie die gewünschte Sicherheitsserver- oder View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .
  c Wählen Sie **[Use PCoIP Secure Gateway for PCoIP connections to desktop (Sicheres PCoIP-Gateway für PCoIP-Verbindungen mit dem Desktop verwenden)]** .

    Das sichere PCoIP-Gateway ist standardmäßig deaktiviert.
  d Stellen Sie sicher, dass im Textfeld **[PCoIP External URL (PCoIP – Externe URL)]** die externe IP-Adresse für die Sicherheitsserver- oder View Connection Server-Instanz angegeben ist, auf die View Client-Instanzen über das Internet zugreifen können.

    Geben Sie Port 4172 an. Schließen Sie keinen Protokollnamen ein.

    Beispiel: **`100.200.300.400:4172`**
  e Stellen Sie sicher, dass es sich sowohl bei der **[externen PCoIP-URL]** als auch bei der **[externen URL]** des sicheren Tunnels um die Adressen handelt, die Clientsysteme zur Verbindungsherstellung mit diesem Host verwenden.

    Geben Sie beispielsweise bei der Konfiguration eines View Connection Server-Hosts weder die **[externe PCoIP-URL]** für diesen Host noch die **[externe URL]** des sicheren Tunnels für einen kombinierten Sicherheitsserver an.
  f Klicken Sie auf **[OK]** .
- Wenn der Benutzer eine Verbindung über einen Webproxy herstellt, der sich außerhalb Ihres Netzwerks befindet und den erforderlichen Port blockiert, weisen Sie den Benutzer an, sich über einen anderen Netzwerkstandort zu verbinden.
- Stellen Sie sicher, dass sowohl der Sicherheitsserver als auch die kombinierte View Connection Server-Instanz View 4.6 oder eine höhere Version verwenden.

Verbindungsprobleme zwischen Desktops und View Connection Server-Instanzen

Bei der Verbindung zwischen Desktops und View Connection Server-Instanzen können Probleme auftreten.

Problem

Wenn für die Konnektivität zwischen einem Desktop und einer View Connection Server-Instanz ein Fehler auftritt, wird in der Ereignisdatenbank eine der folgenden Meldungen angezeigt.

- `Provisioning error occurred for Machine` *`Name_der_Maschine`*`: Customization error due to no network communication between the View agent and Connection Server (Bereitstellungsfehler für Maschine` *`Name_der_Maschine`*`: Anpassungsfehler, da keine Netzwerkkommunikation zwischen der View Agent- und Connection Server-Instanz möglich ist)`
- `Provisioning error occurred on Pool` *`Desktop-ID`* `because of a networking problem with a View Agent (Bereitstellungsfehler für Pool` *`Desktop-ID`* `aufgrund eines Netzwerkproblems mit einer View Agent-Instanz)`
- `Unable to launch from Pool` *`Desktop-ID`* `for user` *`Anzeigename_des_Benutzers`*`: Failed to connect to Machine` *`Name_der_Maschine`* `using` *`Protokoll`* `(Starten aus Pool` *`Desktop-ID`* `für Benutzer` *`Anzeigename_des_Benutzers`* `nicht möglich: Verbindung zu Maschine` *`Name_der_Maschine`* `konnte unter Verwendung von` *`Protokoll`* `nicht hergestellt werden)`

Ursache

Bei der Konnektivität zwischen einem Desktop und einer View Connection Server-Instanz können aus verschiedenen Gründen Probleme auftreten.

- Lookup-Fehler auf dem Desktop für den DNS-Namen des View Connection Server-Hosts.
- Die Ports für die JMS-, RDP- oder AJP13-Kommunikation werden durch Firewall-Regeln blockiert.
- Ein Ausfall des JMS-Routers auf dem View Connection Server-Host.

Lösung

- Geben Sie an einer Eingabeaufforderung auf dem Desktop den Befehl `nslookup` ein.

  `nslookup` *`CS-FQDN`*

  CS-FQDN ist der vollqualifizierte Domänenname (FQDN) des View Connection Server-Hosts. Wenn der Befehl die IP-Adresse des View Connection Server-Hosts nicht zurückgibt, korrigieren Sie die DNS-Konfiguration mithilfe der allgemeinen Verfahren zur Behandlung von Netzwerkproblemen.

- Stellen Sie an einer Eingabeaufforderung auf dem Desktop sicher, dass TCP-Port 4001 ordnungsgemäß funktioniert. Dieser Port wird von der View Agent-Instanz für die JMS-Kommunikation mit dem View Connection Server-Host verwendet. Geben Sie zu diesem Zweck den `telnet`-Befehl ein.

  `telnet` *`CS-FQDN`* `4001`

  Wenn die `telnet`-Verbindung hergestellt wird, funktioniert die Netzwerkkonnektivität für JMS ordnungsgemäß.

- Wenn ein Sicherheitsserver in der DMZ bereitgestellt wird, stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um RDP-Konnektivität zwischen dem Sicherheitsserver und virtuellen Desktop-Maschinen an TCP-Port 3389 zuzulassen.
- Wenn sichere Verbindungen umgangen werden, stellen Sie sicher, dass die Firewall-Regeln Folgendes zulassen: Clients können eine direkte RDP-Verbindung mit der virtuellen Desktop-Maschine an TCP-Port 3389 oder eine direkte PCoIP-Verbindung mit der virtuellen Desktop-Maschine an TCP-Port 4172 und UDP-Port 4172 herstellen.
- Stellen Sie sicher, dass in der inneren Firewall Ausnahmeregeln konfiguriert sind, um Verbindungen zwischen jeder Security Server-Instanz und dem zugehörigen View Connection Server-Host an TCP-Port 4001 (JMS) und TCP-Port 8009 (AJP13) zuzulassen.

Verbindungsprobleme aufgrund einer falschen Zuweisung von IP-Adressen zu geklonten Desktops

Möglicherweise kann keine Verbindung zu geklonten Desktops hergestellt werden, wenn diese über statische IP-Adressen verfügen.

Problem

View Client kann nicht verwendet werden, um eine Verbindung mit geklonten Desktops herzustellen.

Ursache

Geklonte Desktops sind fälschlicherweise für die Verwendung einer statischen IP-Adresse konfiguriert. Diese Desktops sollten die IP-Adressen jedoch über DHCP abrufen.

Lösung

1 Stellen Sie sicher, dass die Vorlage für einen Desktop-Pool auf einer vCenter-Instanz für die Verwendung von DHCP konfiguriert ist, um IP-Adressen für Desktops zuzuweisen.

2 Klonen Sie in VMware Infrastructure Client eine virtuelle Maschine manuell aus dem Desktop-Pool und stellen Sie sicher, dass die IP-Adresse ordnungsgemäß über DHCP abgerufen wird.

Fehlerbehebung bei Problemen während der Desktop-Pool-Erstellung

Für die Diagnose und Behandlung von Problemen bei der Erstellung von Desktop-Pools gibt es mehrere Vorgehensweisen.

Fehler bei der Pool-Erstellung, wenn keine Anpassungsspezifikationen gefunden werden

Beim Versuch, einen Desktop-Pool zu erstellen, schlägt der Vorgang fehl, wenn die Anpassungsspezifikationen nicht gefunden werden können.

Problem

Sie können keinen Desktop-Pool erstellen und Ihnen wird die folgende Nachricht in der Ereignisdatenbank angezeigt.

`Provisioning error occurred for Machine` *`Name_der_Maschine`*`: Customization failed for Machine (Bereitstellungsfehler für Maschine` *`Name_der_Maschine`*`: Anpassung für Maschine fehlgeschlagen)`

Ursache

Die Ursache dieses Problems ist wahrscheinlich, dass Sie nicht über ausreichende Berechtigungen verfügen, um auf die Anpassungsspezifikationen zuzugreifen oder einen Pool zu erstellen. Eine weitere mögliche Ursache ist, dass die Anpassungsspezifikation umbenannt oder gelöscht wurde.

Lösung

- Stellen Sie sicher, dass Sie über ausreichend Berechtigungen für den Zugriff auf die Anpassungsspezifikationen und die Erstellung eines Pools verfügen.
- Wenn die Anpassungsspezifikation nicht mehr vorhanden ist, da sie umbenannt oder gelöscht wurde, wählen Sie eine andere Spezifikation.

Fehler bei der Pool-Erstellung aufgrund eines Berechtigungsproblems

Sie können keinen Desktop-Pool erstellen, wenn ein Berechtigungsproblem mit einem ESX/ESXi-Host, ESX/ESXi-Cluster oder Rechenzentrum vorliegt.

Problem

In View Administrator kann kein Desktop-Pool erstellt werden, da kein Zugriff auf die Vorlagen, den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum möglich ist.

Ursache

Dieses Problem kann verschiedene Ursachen haben.

- Sie verfügen nicht über die erforderlichen Berechtigungen zum Erstellen eines Pools.
- Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf die Vorlagen.
- Sie verfügen nicht über die erforderlichen Berechtigungen für den Zugriff auf den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum.

Lösung

- Wenn im Fenster zur Vorlagenauswahl keine verfügbaren Vorlagen angezeigt werden, stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf die Vorlagen verfügen.

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf den ESX/ESXi-Host, den ESX/ESXi-Cluster oder das Rechenzentrum verfügen.
- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für das Erstellen eines Pools verfügen.

Fehler bei der Pool-Bereitstellung aufgrund eines Konfigurationsproblems

Wenn eine Vorlage nicht verfügbar ist oder das Image einer virtuellen Maschine verschoben oder gelöscht wurde, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

Problem

Es wird kein Desktop-Pool bereitgestellt und Ihnen wird die folgende Meldung in der Ereignisdatenbank angezeigt.

`Provisioning error occurred on Pool` *`Desktop-ID`* `because of a configuration problem (Bereitstellungsfehler aufgrund eines Konfigurationsproblems für Pool` *`Desktop-ID`*`)`

Ursache

Dieses Problem kann verschiedene Ursachen haben.

- Der Zugriff auf eine Vorlage ist nicht möglich.
- Der Name einer Vorlage wurde in vCenter geändert.
- Eine Vorlage wurde in vCenter in einen anderen Ordner verschoben.
- Das Image einer virtuellen Maschine wurde zwischen ESX/ESXi-Hosts verschoben oder gelöscht.

Lösung

- Stellen Sie sicher, dass der Zugriff auf die Vorlage möglich ist.
- Stellen Sie sicher, dass der richtige Name und Ordner für die Vorlage angegeben wird.
- Wenn das Image einer virtuellen Maschine zwischen ESX/ESXi-Hosts verschoben wurde, verschieben Sie die virtuelle Maschine in den richtigen vCenter-Ordner.
- Wenn das Image einer virtuellen Maschine gelöscht wurde, löschen Sie den Eintrag für die virtuelle Maschine in View Administrator und erstellen Sie das Image neu bzw. stellen Sie das Image wieder her.

Fehler bei der Pool-Bereitstellung, da eine View Connection Server-Instanz keine Verbindung mit einer vCenter-Instanz herstellen kann

Wenn eine View Connection Server-Instanz keine Verbindung mit einer vCenter-Instanz herstellen kann, schlägt die Bereitstellung eines Desktop-Pools möglicherweise fehl.

Problem

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird eine der folgenden Fehlermeldungen in der Ereignisdatenbank angezeigt.

- `Cannot log in to vCenter at address` *`VC-Adresse`* `(Anmeldung an vCenter bei Adresse` *`VC-Adresse`* `nicht möglich)`
- `The status of vCenter at address` *`VC-Adresse`* `is unknown (Der Status von vCenter bei Adresse` *`VC-Adresse`* `ist unbekannt)`

Ursache

Die View Connection Server-Instanz kann aus einem der folgenden Gründe keine Verbindung zur vCenter-Instanz herstellen.

- Der Webdienst auf der vCenter Server-Instanz wurde angehalten.

- Zwischen dem View Connection Server-Host und der vCenter Server-Instanz sind Netzwerkprobleme aufgetreten.
- Die Portnummern und Anmeldeinformationen für vCenter oder View Composer haben sich geändert.

Lösung

- Stellen Sie sicher, dass der Webdienst auf der vCenter-Instanz ausgeführt wird.
- Stellen Sie sicher, dass zwischen dem View Connection Server-Host und der vCenter-Instanz keine Netzwerkprobleme aufgetreten sind.
- Überprüfen Sie in View Administrator die Portnummern und Anmeldeinformationen, die für vCenter und View Composer konfiguriert sind.

Fehler bei der Pool-Bereitstellung aufgrund von Datenspeicherproblemen

Wenn der Festplattenspeicherplatz eines Datenspeichers belegt ist oder Sie nicht für den Zugriff auf den Datenspeicher berechtigt sind, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

Problem

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird eine der folgenden Fehlermeldungen in der Ereignisdatenbank angezeigt.

- `Provisioning error occurred for Machine Name_der_Maschine: Cloning failed for Machine (Bereitstellungsfehler für Maschine Name_der_Maschine: Klonen der Maschine fehlgeschlagen)`
- `Provisioning error occurred on Pool Desktop-ID because available free disk space is reserved for linked clones (Bereitstellungsfehler für Pool Desktop-ID, da verfügbarer Speicherplatz für verknüpfte Klone reserviert ist)`
- `Provisioning error occurred on Pool Desktop-ID because of a resource problem (Bereitstellungsfehler aufgrund eines Ressourcenproblems für Pool Desktop-ID)`

Ursache

Sie sind nicht für den Zugriff auf den ausgewählten Datenspeicher berechtigt oder der für den Pool verwendete Datenspeicher ist belegt.

Lösung

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen für den Zugriff auf den ausgewählten Datenspeicher verfügen.
- Überprüfen Sie, ob die Festplatte, auf welcher der Datenspeicher konfiguriert ist, voll ist.
- Wenn die Festplatte voll oder der Speicherplatz reserviert ist, geben Sie Speicherplatz frei, verteilen Sie die verfügbaren Datenspeicher neu oder migrieren Sie den Datenspeicher auf eine Festplatte mit höherer Kapazität.

Fehler bei der Pool-Bereitstellung, da eine vCenter-Instanz überlastet ist

Wenn vCenter durch das Volumen an Anforderungen überlastet ist, kann die Bereitstellung eines Desktop-Pools fehlschlagen.

Problem

Die Bereitstellung eines Desktop-Pools schlägt fehl und Ihnen wird die folgende Fehlermeldung in der Ereignisdatenbank angezeigt.

`Provisioning error occurred on Pool Desktop-ID because of a timeout while customizing (Bereitstellungsfehler aufgrund einer Zeitüberschreitung bei der Anpassung für Pool Desktop-ID)`

Ursache

vCenter ist durch das Volumen an Anforderungen überlastet.

Lösung

- Verringern Sie in View Administrator die maximale Anzahl gleichzeitig ausgeführter Bereitstellungs- und Betriebsvorgänge für vCenter.
- Konfigurieren Sie zusätzliche vCenter Server-Instanzen.

  Weitere Informationen zur Konfiguration von vCenter finden Sie im Dokument *Installation von VMware View*.

Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen

Nach dem Klonen verlassen virtuelle Maschinen den Bereitstellungsstatus nicht.

Problem

Virtuelle Maschinen können den Bereitstellungsstatus nicht verlassen.

Ursache

Die Ursache dieses Problems ist wahrscheinlich, dass Sie die View Connection Server-Instanz während eines Klonvorgangs neu gestartet haben.

Lösung

- Löschen Sie die virtuellen Maschinen und führen Sie den Klonvorgang erneut aus.

Virtuelle Maschinen können den Anpassungsstatus nicht verlassen

Nach dem Klonen verlassen virtuelle Maschinen den Anpassungsstatus nicht.

Problem

Virtuelle Maschinen können den Anpassungsstatus nicht verlassen.

Ursache

Die Ursache für dieses Problem ist wahrscheinlich, dass nicht genügend Festplattenspeicherplatz zum Starten der virtuellen Maschine verfügbar ist. Bevor eine Anpassung durchgeführt werden kann, muss eine virtuelle Maschine gestartet werden.

Lösung

- Löschen Sie die virtuelle Maschine, um eine Wiederherstellung durchzuführen, wenn eine Maschine den Anpassungsstatus nicht verlassen kann.
- Wenn die Festplatte voll ist, geben Sie Speicherplatz frei oder migrieren Sie den Datenspeicher auf eine Festplatte mit höherer Kapazität.

Fehlerbehebung bei Problemen mit der USB-Umleitung

Bei der USB-Umleitung in View Client können verschiedene Probleme auftreten.

Problem

Bei der USB-Umleitung in View Client werden lokale Geräte nicht auf dem Remote-Desktop verfügbar gemacht oder einige Geräte werden für die Umleitung in View Client nicht als verfügbar angezeigt.

Ursache

Im Folgenden sind mögliche Ursachen aufgeführt, aufgrund derer die USB-Umleitung nicht ordnungsgemäß oder wie erwartet ausgeführt werden kann.

- Die USB-Umleitung wird für Windows 2003-Systeme oder Windows 2008-Systeme oder für von Microsoft-Terminaldiensten verwaltete View-Desktops nicht unterstützt.
- Die Umleitung wird für Webcams nicht unterstützt.
- Die Umleitung von USB-Audiogeräten hängt vom Status des Netzwerks ab und ist nicht zuverlässig. Einige Geräte erfordern selbst dann einen hohen Datendurchsatz, wenn sie sich im Leerlauf befinden.
- Die USB-Umleitung wird für Startgeräte nicht unterstützt. Wenn Sie View Client auf einem Windows-System ausführen, das von einem USB-Gerät startet, und Sie dieses Gerät auf den Remote-Desktop umleiten, reagiert das lokale Betriebssystem möglicherweise nicht oder kann nicht verwendet werden. Siehe http://kb.vmware.com/kb/1021409.
- Die Auswahl von Eingabe- und Bluetooth-Geräten, die mit einem Eingabegerät zur Umleitung kombiniert werden, ist bei View Client für Windows standardmäßig nicht zulässig. Siehe http://kb.vmware.com/kb/1011600.
- RDP bietet keine Unterstützung für die Umleitung von USB-Eingabegeräten für die Konsolensitzung oder für Smartcard-Leser. Siehe http://kb.vmware.com/kb/1011600.
- RDP kann bei Verwendung von USB-Flashkarten unerwartete Probleme verursachen. Siehe http://kb.vmware.com/kb/1019547.
- Windows Mobile-Gerätecenter kann die Umleitung von USB-Geräten für RDP-Sitzungen verhindern. Siehe http://kb.vmware.com/kb/1019205.
- Für einige USB-Eingabegeräte müssen Sie die virtuelle Maschine so konfigurieren, dass die Position des Mauszeigers aktualisiert wird. Siehe http://kb.vmware.com/kb/1022076.
- Einige Audiogeräte erfordern möglicherweise Änderungen an Richtlinieneinstellungen oder Registrierungseinstellungen. Siehe http://kb.vmware.com/kb/1023868.
- Netzwerklatenz kann zu einer langsamen Geräteinteraktion führen. Zudem ist es möglich, dass Anwendungen nicht zu reagieren scheinen, da sie für die Interaktion mit lokalen Geräten konzipiert sind. Bei USB-Festplattenlaufwerken mit sehr hoher Kapazität kann es einige Minuten dauern, bis diese im Windows Explorer angezeigt werden.
- USB-Flashkarten, die mit dem FAT32-Dateisystem formatiert sind, werden langsam geladen. Siehe http://kb.vmware.com/kb/1022836.
- Ein Prozess oder Dienst auf dem lokalen System hat das Gerät geöffnet, bevor Sie sich mit dem Remote-Desktop verbunden haben.
- Ein umgeleitetes USB-Gerät arbeitet nicht mehr, wenn Sie eine Desktop-Sitzung wiederherstellen – selbst wenn der Desktop anzeigt, dass das Gerät verfügbar ist.
- Die USB-Umleitung ist in View Administrator deaktiviert.
- Fehlende oder deaktivierte Treiber für die USB-Umleitung auf dem Gast.
- Fehlende oder deaktivierte Treiber für die USB-Umleitung bzw. fehlende oder deaktivierte Treiber für das Gerät, das umgeleitet werden soll, auf dem Client.

Lösung

- Verwenden Sie, wenn möglich, PCoIP anstelle von RDP als Desktop-Protokoll.
- Wenn ein umgeleitetes Gerät weiterhin nicht verfügbar ist oder nach einer vorübergehenden Verbindungstrennung nicht mehr arbeitet, entfernen Sie das Gerät, schließen Sie es wieder an, und führen Sie erneut eine Umleitung durch.

- Wechseln Sie in View Administrator zu **[Policies (Richtlinien)] > [Global Policies (Globale Richtlinien)]** , und stellen Sie sicher, dass für den USB-Zugriff unter **[View Policies (Richtlinien anzeigen)]** die Option „Allow (Zulassen)“ festgelegt ist.
- Überprüfen Sie das Protokoll auf dem Gast auf Einträge der Klasse `wssm_usb` und das Protokoll auf dem Client auf Einträge der Klasse `wswc_usb`.

  Einträge dieser Klassen werden in die Protokolle geschrieben, wenn es sich bei einem Benutzer nicht um einen Administrator handelt oder wenn die Treiber für die USB-Umleitung nicht installiert sind oder nicht ordnungsgemäß funktionieren.
- Öffnen Sie auf dem Gast den Geräte-Manager, erweitern Sie die USB-Controller und installieren Sie die Treiber VMware View Virtual USB Device Manager und VMware View Virtual USB Hub erneut, wenn diese Treiber nicht vorhanden sind, bzw. aktivieren Sie die Treiber, wenn diese deaktiviert sind.
- Öffnen Sie auf dem Client den Geräte-Manager, erweitern Sie die USB-Controller und installieren Sie den Treiber „VMware View Generic USB Device“ und den USB-Treiber für das umgeleitete Gerät erneut, wenn diese Treiber nicht vorhanden sind, bzw. aktivieren Sie die Treiber, wenn diese deaktiviert sind.

Beheben von Fehlern bei der QuickPrep-Anpassung

Ein View Composer QuickPrep-Anpassungsskript kann aus verschiedenen Gründen fehlschlagen.

Problem

Ein nach der Synchronisierung ausgeführtes QuickPrep-Skript oder Abschaltskript wird nicht ausgeführt. In einigen Fällen wird ein Skript für einige verknüpfte Klone möglicherweise vollständig ausgeführt, auf anderen Klonen schlägt es jedoch fehl.

Ursache

Häufige Ursachen für QuickPrep-Skriptfehler sind:

- Zeitüberschreitung bei der Skriptausführung
- Der Skriptpfad bezieht sich auf ein Skript, das einen Interpreter erfordert
- Das für die Ausführung des Skripts verwendete Konto verfügt nicht über ausreichende Berechtigungen, um eine Skriptaufgabe auszuführen

Lösung

- Überprüfen Sie das Protokoll des Anpassungsskripts.

  Die Informationen zur QuickPrep-Anpassung werden in eine Protokolldatei im Windows-Verzeichnis `temp` geschrieben:

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```
- Überprüfen Sie, ob bei der Skriptausführung eine Zeitüberschreitung aufgetreten ist.

  View Composer beendet ein Anpassungsskript, wenn dessen Ausführung länger als 20 Sekunden dauert. In der Protokolldatei wird in einer Meldung angezeigt, dass das Skript gestartet wurde, in einer weiteren Meldung wird die Zeitüberschreitung angezeigt:

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script: cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  Um ein Zeitüberschreitungsproblem zu beheben, erhöhen Sie das Zeitüberschreitungslimit für das Skript und führen Sie es erneut aus.

- Überprüfen Sie, ob der Skriptpfad gültig ist.

  Wenn Sie eine Skriptsprache verwenden, die zur Skriptausführung einen Interpreter erfordert, muss der Skriptpfad mit der Interpreter-Binärdatei beginnen.

  Wenn Sie beispielsweise den Pfad `C:\script\myvb.vbs` als QuickPrep-Anpassungsskript angeben, kann View Composer Agent das Skript nicht ausführen. Sie müssen einen Pfad angeben, der mit der Interpreter-Binärdatei beginnt:

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- Überprüfen Sie, ob das für die Ausführung des Skripts verwendete Konto über die erforderlichen Berechtigungen zur Ausführung von Skriptaufgaben verfügt.

  QuickPrep führt die Skripts mit dem Konto aus, das zur Ausführung des VMware View Composer Gastagentserver-Dienstes konfiguriert ist. Standardmäßig handelt es sich hier um das Konto `Local System (Lokales System)`.

  Ändern Sie dieses Anmeldekonto nicht. Wenn Sie das Konto ändern, können die verknüpften Klone nicht starten.

View Composer-Bereitstellungsfehler

Wenn bei der Bereitstellung oder Neuzusammenstellung von Linked-Clone-Desktops durch View Composer ein Fehler auftritt, wird die Fehlerursache durch einen Fehlercode angezeigt. Der Fehlercode wird in View Administrator in der Spalte mit dem Desktop-Status angezeigt.

Tabelle 16-2 beschreibt die View Composer-Bereitstellungsfehlercodes.

In dieser Tabelle werden Fehler im Zusammenhang mit View Composer- und QuickPrep-Anpassungen aufgeführt. In View Connection Server und anderen View-Komponenten können weitere Fehler auftreten, die möglicherweise zu Problemen bei der Desktop-Bereitstellung führen.

Tabelle 16-2. View Composer-Bereitstellungsfehler

Error (Fehler)	Beschreibung
0	Die Richtlinie wurde erfolgreich angewendet. **Hinweis** Der Ergebniscode 0 wird in View Administrator nicht angezeigt. Der Linked-Clone-Desktop wechselt in den Status **[Ready (Bereit)]** , sofern nicht ein View Manager-Fehler außerhalb der View Composer-Domäne auftritt. Dieser Ergebniscode ist der Vollständigkeit halber enthalten.
1	Der Computername konnte nicht festgelegt werden.
2	Die Benutzerprofile konnten nicht an die persistente View Composer-Festplatte umgeleitet werden.
3	Das Domänenkontokennwort des Computers konnte nicht festgelegt werden.
4	Die Profilschlüssel eines Benutzers konnten nicht gesichert werden. Bei der nächsten Anmeldung des Benutzers an diesem Linked-Clone-Desktop nach der Neuzusammenstellung erstellt das Betriebssystem ein neues Profilverzeichnis für den Benutzer. Da ein neues Profil erstellt wird, kann der Benutzer die alten Profildaten nicht anzeigen.
5	Ein Benutzerprofil konnte nicht wiederhergestellt werden. Der Benutzer sollte sich bei diesem Status nicht am Desktop anmelden, da der Profilstatus nicht definiert ist.

Tabelle 16-2. View Composer-Bereitstellungsfehler (Fortsetzung)

Error (Fehler)	Beschreibung
6	Fehler, die nicht durch andere Fehlercodes abgedeckt werden. Die View Composer Agent-Protokolldateien im Gastbetriebssystem umfassen möglicherweise weitere Informationen zu den Ursachen dieser Fehler. Beispielsweise kann dieser Fehlercode durch eine Windows PnP-Zeitüberschreitung (Plug and Play) generiert werden. In dieser Situation kommt es für View Composer zu einer Zeitüberschreitung, während auf die Installation neuer Volumes für die virtuelle Linked-Clone-Maschine durch den PnP-Dienst gewartet wird. PnP mountet abhängig von der Pool-Konfiguration bis zu drei Festplatten: ■ Persistente View Composer-Festplatte ■ Nicht persistente Festplatte zum Umleiten von temporären und Auslagerungsdateien des Gastbetriebssystems ■ Interne Festplatte zum Speichern der QuickPrep-Konfiguration und anderer betriebssystembezogener Daten. Diese Festplatte wird immer mit einem verknüpften Klon konfiguriert. Der für die Zeitüberschreitung definierte Wert lautet 10 Minuten. Wenn das Mounten der Festplatten durch PnP nicht innerhalb von 10 Minuten abgeschlossen wird, schlägt View Composer mit dem Fehlercode 6 fehl.
7	Eine zu große Anzahl an persistenten View Composer-Festplatten ist mit dem verknüpften Klon verbunden. Ein Klon kann über maximal drei persistente View Composer-Festplatten verfügen.
8	Eine persistente Festplatte konnte nicht in dem bei der Pool-Erstellung ausgewählten Datenspeicher gemountet werden.
9	View Composer konnte Dateien mit löschbaren Daten nicht auf die nicht persistente Festplatte umleiten. Die Auslagerungsdatei oder die Ordner mit temporären Dateien wurden nicht umgeleitet.
10	View Composer kann die QuickPrep-Konfigurationsrichtliniendatei auf der angegebenen internen Festplatte nicht finden.
12	View Composer kann die interne Festplatte mit der QuickPrep-Konfigurationsrichtliniendatei und andere betriebssystembezogene Daten nicht finden.
13	Mehrere persistente Festplatten sind für die Umleitung des Windows-Benutzerprofils konfiguriert.
14	View Composer konnte die interne Festplatte nicht unmounten.
15	Der Computername, den View Composer aus der Konfigurationsrichtliniendatei gelesen hat, stimmt nach dem anfänglichen Einschalten des verknüpften Klons nicht mit dem aktuellen Systemnamen überein.
16	View Composer Agent wurde nicht gestartet, da die Volumelizenz für das Gastbetriebssystem nicht aktiviert wurde.
17	View Composer Agent wurde nicht gestartet. Für den Agenten ist es beim Warten auf den Sysprep-Start zu einer Zeitüberschreitung gekommen.
18	View Composer Agent konnte die virtuelle Linked-Clone-Maschine während der Anpassung nicht mit einer Domäne verknüpfen.
19	Der View Composer-Agent konnte das nach der Synchronisierung auszuführende Skript nicht anwenden.
20	Der View Composer-Agent konnte ein Synchronisierungsereignis für ein Computerkennwort nicht bearbeiten. Es handelt sich hier möglicherweise um einen vorübergehenden Fehler. Kann der verknüpfte Klon zur Domäne hinzugefügt werden, ist das Passwort in Ordnung. Kann der Klon nicht zur Domäne hinzugefügt werden, muss der Vorgang neu gestartet werden, den Sie vor Auftreten des Fehlers durchgeführt haben. Falls Sie den Klon neu gestartet haben, sollten Sie dies erneut tun. Falls Sie den Klon aktualisiert haben, sollten Sie dies erneut tun. Kann der Klon immer noch nicht zur Domäne hinzugefügt werden, muss er neu zusammengestellt werden.

Fehler beim Hinzufügen von verknüpften Windows XP-Klonen zur Domäne

Linked-Clone-Desktops mit Windows XP können möglicherweise nicht zur Domäne hinzugefügt werden, wenn Active Directory unter Windows Server 2008 ausgeführt wird.

Problem

Bei der Bereitstellung von Linked-Clone-Desktops können die verknüpften Klone nicht zur Domäne hinzugefügt werden. View Administrator zeigt die View Composer-Bereitstellungsfehlermeldungen an. Beispiel:

```
5/17/10 3:11:50 PM PDT: View Composer agent initialization state error (18): Failed to join the domain (waited 565 seconds) (Statusfehler bei View Composer Agent–Initialisierung (18): Beitreten zur Domäne fehlgeschlagen [565 Sekunden gewartet])
```

Ursache

Dieses Problem kann auftreten, wenn Active Directory unter Windows Server 2008 ausgeführt wird. Der schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC) in Windows Server 2008 ist nicht mit virtuellen Windows XP-Maschinen abwärtskompatibel.

Lösung

1 Überprüfen Sie das View Composer-Protokoll auf die folgende Fehlermeldung:

```
0x4f1: The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you. (Das System hat eine mögliche Sicherheitsgefahr festgestellt. Stellen Sie sicher, dass Sie mit dem Server, der Sie authentifiziert hat, Verbindung aufnehmen können.)
```

Die View Composer-Protokolldatei wird standardmäßig im Windows-Verzeichnis `Temp` generiert: `C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

2 Spielen Sie auf der übergeordneten virtuellen Maschine das Windows Server 2008-RODC-Kompatibilitäts-Update für Windows XP auf.

Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 944043 unter: http://support.microsoft.com/kb/944043/en-us.

3 Erstellen Sie einen Snapshot der aktualisierten übergeordneten virtuellen Maschine.

4 Stellen Sie die Linked-Clone-Desktops aus der aktualisierten übergeordneten virtuellen Maschine und dem Snapshot neu zusammen.

Fehlerbehebung von GINA-Problemen auf Windows XP-Desktops

Auf Windows XP-Desktops können bei der Verkettung von VMware View Graphical Identification and Authentication (GINA, Grafische Identifizierung und Authentifizierung) Probleme auftreten Dateien der Dynamic Link Library (dll).

Problem

Auf Windows XP-Desktops können die folgenden Probleme auftreten:

- Der Desktop startet nicht
- Beim Start oder Herunterfahren eines Desktops wird der folgende Fehler angezeigt: `Cannot start gina.dll module (GINA-dll-Modul kann nicht gestartet werden). A required component is missing (Es fehlt eine erforderliche Komponente): gina.dll. Please install the application again (gina.dll. Installieren Sie die Anwendung erneut).`

- Beim Start eines Desktops wird eine unerwartete Anmeldeaufforderung angezeigt
- Sie können sich nicht am Desktop anmelden

Ursache

Probleme beim Start und bei der Anmeldung können auf Windows XP-Desktops auftreten, wenn die View GINA-`dll`-Dateien nicht korrekt mit den Drittanbieter-GINAs verkettet werden, die sich eventuell auf den virtuellen Maschinen befinden.

Um sicherzustellen, dass die GINA korrekt verkettet wurde, müssen Sie die GINA `WinLogon` als View-GINA konfigurieren und dafür sorgen, dass `vdmGinaChainDLL` erstellt wurde und die Drittanbieter-GINAs enthält.

Wenn Sie keine Software installiert haben, die eine Verkettung zu einer anderen GINA herstellt, ist `msgina.dll` als Standard eingestellt und befindet sich unter `%systemroot%\system32\msgina.dll` auf der virtuellen Maschine.

Lösung

1 Melden Sie sich an der übergeordneten virtuellen Maschine, der virtuellen Vorlagenmaschine oder am View-Desktop an.

2 Klicken Sie auf **[Start] > [Run (Ausführen)]**, geben Sie **`Regedit`** ein und drücken Sie auf die Eingabetaste.

3 Navigieren Sie zum folgenden Windows-Registrierungsschlüssel:

```
HKEY_LOKALE_MASCHINE\Software\Microsoft\Windows NT\Aktuelle Version\Winlogon\GinaDLL
```

4 Stellen Sie sicher, dass der Schlüssel `GinaDLL` den folgenden Wert aufweist:

Installationsverzeichnis\VMware\VMware View\Agent\bin\wsgina.dll

Installationsverzeichnis ist der Pfad, unter dem Sie View Agent installiert haben.

5 Ist der Zeichenfolgewert `vdmGinaChainDLL` nicht vorhanden, müssen Sie diesen erstellen.

a Navigieren Sie zum folgenden Registrierungsschlüssel:

```
HKEY_LOKALE_MASCHINE\Software\Microsoft\Windows NT\AktuelleVersion
```

b Erstellen Sie den Schlüssel `vdmGinaChainDLL`.

6 Legen Sie die `dll`-Namen der Drittanbieter-GINA im Schlüssel `vdmGinaChainDLL` ab.

7 Falls danach immer noch Probleme bei den Windows XP-Desktops auftreten, sollten Sie sicherstellen, dass keine herstellerspezifischen GINA-Schlüssel in der Registrierung geladen werden.

Beim Laden von Drittanbieter-GINA-Schlüsseln ruft die verkettende GINA eventuell immer noch die Standard-GINA `msgina` auf. Manche Netzwerkmanagement- und Sicherheitssoftware-Produkte legen ihre GINA-Ersatz-`dlls` in ihren eigenen Installationsverzeichnissen ab, zum Beispiel unter Registrierungspfaden wie diesem:

```
HKEY_LOKALE_MASCHINE\Software\Anbieter-ID_oder_-Name\GINA-Schlüsselreferenz\GINA-_Ladebefehle
= msgina
```

Entfernen Sie diese GINA-Schlüssel aus dem herstellerspezifischen Speicherort und legen Sie sie im Schlüssel `vdmGinaChainDLL` ab.

17 Verwenden des Befehls „vdmadmin“

Über den Befehl `vdmadmin` kann eine Vielzahl von Verwaltungsaufgaben für eine View Connection Server-Instanz ausgeführt werden.

Mithilfe von `vdmadmin` ist das Ausführen von Verwaltungsaufgaben möglich, die nicht über die View Administrator-Benutzeroberfläche ausgeführt werden können oder die automatisch über Skripts ausgeführt werden müssen.

Einen Vergleich der Vorgänge, die Sie mit View Administrator, View-Cmdlets und `vdmadmin` durchführen können, finden Sie im Dokument *Integration von VMware View*.

- Verwendung des Befehls „vdmadmin“ auf Seite 383

  Die Syntax des Befehls `vdmadmin` bestimmt seine Ausführung.

- Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“ auf Seite 385

  Sie können den Befehl `vdmadmin` mit der Option `–A` verwenden, um die Protokollierung in View Agent zu konfigurieren.

- Außerkraftsetzen von IP-Adressen unter Verwendung der Option „-A“ auf Seite 387

  Sie können den Befehl `vdmadmin` mit der Option `–A` verwenden, um die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

- Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C“ auf Seite 388

  Sie können den Befehl `vdmadmin` mit der Option `–C` verwenden, um den Namen einer View Connection Server-Gruppe festzulegen. Zur Identifizierung der Gruppe in Microsoft System Center Operations Manager (SCOM) wird dieser Name in der SCOM-Konsole angezeigt.

- Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“ auf Seite 388

  Mithilfe des Befehls `vdmadmin` können über die Option `–F` die fremden Sicherheitsprinzipale (Foreign Security Principals, FSPs) von Windows-Benutzern in Active Directory aktualisiert werden, die für die Verwendung eines Desktops berechtigt sind.

- Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H“ auf Seite 389

  Mithilfe der Option `–H` des Befehls `vdmadmin` können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für View Manager-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

- Auflisten und Anzeigen von Berichten zum View Manager-Betrieb unter Verwendung der Option „-I“ auf Seite 390

  Sie können den Befehl `vdmadmin` mit der Option `–I` verwenden, um die verfügbaren Berichte zum View Manager-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

- Zuweisen von dedizierten Desktops unter Verwendung der Option „-L“ auf Seite 391

  Mithilfe des Befehls `vdmadmin` können Sie über die Option –L Benutzern Desktops aus einem dedizierten Pool zuweisen.

- Anzeigen von Informationen zu Maschinen unter Verwendung der Option „-M“ auf Seite 392

  Sie können den Befehl `vdmadmin` mit der Option –M verwenden, um Informationen zur Konfiguration virtueller Maschinen oder physischer Computer anzuzeigen.

- Konfigurieren von Domänenfiltern unter Verwendung der Option „-N“ auf Seite 393

  Sie können den Befehl `vdmadmin` mit der Option –N zum Steuern der Domänen verwenden, die View Manager für die Endbenutzer zur Verfügung stellt.

- Konfigurieren von Domänenfiltern auf Seite 396

  Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine View Connection Server-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

- Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“ auf Seite 400

  Sie können den Befehl `vdmadmin` mit den Optionen –O und –P verwenden, um die Desktops und Richtlinien von Benutzern anzuzeigen, die nicht länger für die Verwendung des Systems berechtigt sind.

- Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q“ auf Seite 401

  Unter Verwendung des Befehls `vdmadmin` mit der Option –Q können Standardwerte festgelegt und Konten für Clients im Kiosk-Modus erstellt werden, um die Authentifizierung für diese Clients zu aktivieren und Informationen zu ihrer Konfiguration anzuzeigen.

- Anzeigen des ersten Benutzers eines Desktops unter Verwendung der Option „-R“ auf Seite 405

  Sie können den Befehl `vdmadmin` mit der Option –R verwenden, um die anfängliche Zuweisung eines verwalteten Desktops zu ermitteln. Bei Verlust von LDAP-Daten wird diese Information z.B. möglicherweise benötigt, um eine Neuzuweisung von Desktops zu Benutzern durchzuführen.

- Entfernen des Eintrags für eine View Connection Server-Instanz unter Verwendung der Option „-S“ auf Seite 406

  Sie können den Befehl `vdmadmin` mit der Option –S verwenden, um den Eintrag für eine View Connection Server-Instanz aus der View Manager-Konfiguration zu entfernen.

- Festlegen einer maximalen Größe für Paketdateien mithilfe der Option „-T“, um View Transfer Server-Pakete bei der Veröffentlichung zu unterteilen auf Seite 407

  Sie können über den Befehl `vdmadmin` mit der Option –T eine maximale Größe festlegen, ab der View Transfer Server-Pakete bei der Veröffentlichung unterteilt werden. Sie sollten einen Grenzwert festlegen, wenn Sie einen Proxy-Cache verwenden, für den eine maximale Objektgröße definiert ist.

- Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“ auf Seite 407

  Sie können den Befehl `vdmadmin` mit der Option –U verwenden, um detaillierte Informationen zu Benutzern anzuzeigen.

- Entschlüsseln der virtuellen Maschine eines lokalen Desktops unter Verwendung der Option „-V“ auf Seite 408

  VMware View schützt die virtuelle Maschine eines lokalen Desktops, indem das zugehörige Basis-Image verschlüsselt wird. Wenn es nicht möglich ist, den lokalen Desktop einzuschalten oder einzuchecken, können Sie den Befehl `vdmadmin` mit der Option –V dazu verwenden, die virtuelle Maschine zu entschlüsseln, um Daten aus dieser wiederherzustellen.

- Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V“ auf Seite 409

  Sie können den Befehl `vdmadmin` mit der Option –V verwenden, um virtuelle Maschinen im Rechenzentrum zu sperren oder zu entsperren.

- Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“ auf Seite 410

  Sie können den Befehl `vdmadmin` mit der Option –X verwenden, um Konflikte bei LDAP-Einträgen auf replizierten View Connection Server-Instanzen in einer Gruppe zu ermitteln und zu lösen.

Verwendung des Befehls „vdmadmin“

Die Syntax des Befehls `vdmadmin` bestimmt seine Ausführung.

Verwenden Sie den Befehl `vdmadmin` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

`vdmadmin` *`Befehlsoption`* [*`Zusatzoption Argument`*] `...`

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab.

Der Pfad zur ausführbaren Datei des Befehls `vdmadmin` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie diesen zur Umgebungsvariable *PATH* hinzu.

- Authentifizierung für den Befehl „vdmadmin“ auf Seite 383

  Um eine angegebene Aktion erfolgreich auszuführen, muss der Befehl `vdmadmin` als Benutzer mit der Rolle **Administrators (Administratoren)** ausgeführt werden.

- Ausgabeformat des Befehls „vdmadmin“ auf Seite 383

  Bei einigen Optionen des Befehls `vdmadmin` können Sie das Format der Ausgabeinformationen angeben.

- Optionen des Befehls „vdmadmin“ auf Seite 384

  Über die Befehlsoptionen des Befehls `vdmadmin` wird der Vorgang angegeben, der ausgeführt werden soll.

Authentifizierung für den Befehl „vdmadmin“

Um eine angegebene Aktion erfolgreich auszuführen, muss der Befehl `vdmadmin` als Benutzer mit der Rolle **Administrators (Administratoren)** ausgeführt werden.

Sie können View Administrator verwenden, um einem Benutzer die Rolle **Administrators (Administratoren)** zuzuweisen. Siehe Kapitel 2, „Konfigurieren der rollenbasierten Verwaltungsdelegierung“, auf Seite 27.

Wenn Sie als Benutzer ohne ausreichende Berechtigungen angemeldet sind, können Sie die Option –b verwenden, um den Befehl als Benutzer mit der Rolle **Administrators (Administratoren)** auszuführen. Voraussetzung dafür ist, dass Sie das Kennwort dieses Benutzers kennen. Sie können die Option –b angeben, um den Befehl `vdmadmin` als der angegebene Benutzer in der angegebenen Domäne auszuführen. Für die Option –b gelten folgende äquivalente Verwendungsmöglichkeiten:

–b *`Benutzername Domäne`* [*`Kennwort`* | *]

–b *`Benutzername@Domäne`* [*`Kennwort`* | *]

–b *`Domäne\Benutzername`* [*`Kennwort`* | *]

Wenn Sie anstelle eines Kennworts ein Sternchen (*) angeben, werden Sie zur Eingabe des Kennworts aufgefordert. Mit Ausnahme der Optionen –R und –T kann die Option –b mit sämtlichen Befehlsoptionen verwendet werden.

Ausgabeformat des Befehls „vdmadmin“

Bei einigen Optionen des Befehls `vdmadmin` können Sie das Format der Ausgabeinformationen angeben.

Tabelle 17-1 zeigt einige Optionen des Befehls `vdmadmin` für die Ausgabetextformatierung.

Tabelle 17-1. Optionen für die Auswahl des Ausgabeformats

Option	Beschreibung
`-csv`	Formatiert die Ausgabe als kommagetrennte Werte.
`-n`	Zeigt die Ausgabe unter Verwendung von ASCII (UTF-8)-Zeichen an. Dies ist der Standardzeichensatz für kommagetrennte Werte und Ausgaben im Textformat.
`-w`	Zeigt die Ausgabe unter Verwendung von Unicode (UTF-16)-Zeichen an. Dies ist der Standardzeichensatz für XML-Ausgaben.
`-xml`	Formatiert die Ausgabe als XML.

Optionen des Befehls „vdmadmin“

Über die Befehlsoptionen des Befehls `vdmadmin` wird der Vorgang angegeben, der ausgeführt werden soll.

Tabelle 17-2 zeigt die Befehlsoptionen, die Sie mit dem Befehl `vdmadmin` zum Steuern und Untersuchen von View Manager-Vorgängen verwenden können.

Tabelle 17-2. Optionen des Befehls „vdmadmin“

Option	Beschreibung
`-A`	Steuert die Informationen, die von einer View Agent-Instanz in den entsprechenden Protokolldateien aufgezeichnet werden. Siehe „Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A““, auf Seite 385. Setzt die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft. Siehe „Außerkraftsetzen von IP-Adressen unter Verwendung der Option „-A““, auf Seite 387
`-C`	Legt den Namen einer View Connection Server-Gruppe fest. Siehe „Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C““, auf Seite 388.
`-F`	Aktualisiert die fremden Sicherheitsprinzipale (FSPs) in Active Directory für alle oder die angegebenen Benutzer. Siehe „Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F““, auf Seite 388.
`-H`	Zeigt Informationen zum Zustand für View Manager-Dienste an. Siehe „Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H““, auf Seite 389.
`-I`	Generiert Berichte zu View Manager-Vorgängen. Siehe „Auflisten und Anzeigen von Berichten zum View Manager-Betrieb unter Verwendung der Option „-I““, auf Seite 390.
`-L`	Weist einem Benutzer einem dedizierten Desktop zu oder entfernt eine solche Zuweisung. Siehe „Zuweisen von dedizierten Desktops unter Verwendung der Option „-L““, auf Seite 391.
`-M`	Zeigt Informationen zu einer virtuellen Maschine oder einem physischen Computer an. Siehe „Anzeigen von Informationen zu Maschinen unter Verwendung der Option „-M““, auf Seite 392.
`-N`	Konfiguriert die Domänen, die eine View Connection Server-Instanz oder -Gruppe für View Client-Instanzen verfügbar macht. Siehe „Konfigurieren von Domänenfiltern unter Verwendung der Option „-N““, auf Seite 393.
`-O`	Zeigt die Desktops an, die Benutzern zugewiesen sind, die nicht länger über Berechtigungen für diese Desktops verfügen. Siehe „Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P““, auf Seite 400.
`-P`	Zeigt die Benutzerrichtlinien für Desktops von Benutzern an, die nicht über Berechtigungen verfügen. Siehe „Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P““, auf Seite 400.
`-Q`	Konfiguriert das Konto in Active Directory und in View Manager ein Clientgerät im Kiosk-Modus. Siehe „Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q““, auf Seite 401.
`-R`	Gibt den ersten Benutzer an, der auf einen Desktop zugegriffen hat. Siehe „Anzeigen des ersten Benutzers eines Desktops unter Verwendung der Option „-R““, auf Seite 405.

Tabelle 17-2. Optionen des Befehls „vdmadmin“ (Fortsetzung)

Option	Beschreibung
–S	Entfernt einen Konfigurationseintrag für eine View Connection Server-Instanz aus der Konfiguration von View Manager. Siehe „Entfernen des Eintrags für eine View Connection Server-Instanz unter Verwendung der Option „-S““, auf Seite 406.
–T	Legt die maximale Dateigröße für die Unterteilung von View Transfer Server-Paketen fest. Siehe „Festlegen einer maximalen Größe für Paketdateien mithilfe der Option „-T“, um View Transfer Server-Pakete bei der Veröffentlichung zu unterteilen“, auf Seite 407.
–U	Zeigt Informationen zu einem Benutzer an, einschließlich Desktop-Berechtigungen und ThinApp-Zuweisungen sowie Administratorrollen. Siehe „Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U““, auf Seite 407.
–V	Ermöglicht das Wiederherstellen von Daten von einem lokalen Desktop, indem die zugehörige virtuelle Maschine entschlüsselt wird. Siehe „Entschlüsseln der virtuellen Maschine eines lokalen Desktops unter Verwendung der Option „-V““, auf Seite 408. Entsperrt oder sperrt virtuelle Maschinen für lokale Desktops und View Transfer Server-Instanzen. Siehe „Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V““, auf Seite 409.
–X	Ermittelt und löst Konflikte bei LDAP-Einträgen auf replizierten View Connection Server-Instanzen. Siehe „Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X““, auf Seite 410

Konfigurieren der Protokollierung in View Agent unter Verwendung der Option „-A“

Sie können den Befehl `vdmadmin` mit der Option –A verwenden, um die Protokollierung in View Agent zu konfigurieren.

Syntax

```
vdmadmin –A [–b Authentifizierungsargumente] –getDCT–outfile lokale_Datei –d Desktop –m Maschine

vdmadmin –A [–b Authentifizierungsargumente] –getlogfile Protokolldatei –outfile lokale_Datei –d
Desktop –m Maschine

vdmadmin –A [–b Authentifizierungsargumente] –getloglevel [–xml] –d Desktop [–m Maschine]

vdmadmin –A [–b Authentifizierungsargumente] –getstatus [–xml] –d Desktop [–m Maschine]

vdmadmin –A [–b Authentifizierungsargumente] –getversion [–xml] –d Desktop [–m Maschine]

vdmadmin –A [–b Authentifizierungsargumente] –list [–xml] [–w | –n] –d Desktop –m Maschine

vdmadmin –A [–b Authentifizierungsargumente] –setloglevel Ebene –d Desktop [–m Maschine]
```

Nutzungshinweise

Um den technischen Support von VMware bei der Fehlerbehebung für eine View Agent-Instanz zu unterstützen, können Sie ein DCT-Paket (Data Collection Tool) erstellen. Darüber hinaus können Sie die Protokollierungsebene ändern, die Version und den Status von View Agent anzeigen und einzelne Protokolldateien auf der lokalen Festplatte speichern.

Optionen

Tabelle 17-3 zeigt die verfügbaren Optionen für die Konfiguration der Protokollierung in View Agent.

Tabelle 17-3. Optionen für die Konfiguration der Protokollierung in View Agent

Option	Beschreibung
`–d` *Desktop*	Gibt den Desktop-Pool an.
`–getDCT`	Erstellt ein DCT-Paket (Data Collection Tool) und speichert es in einer lokalen Datei.
`–getlogfile` *Protokolldatei*	Gibt den Namen der Protokolldatei an, für die eine Kopie gespeichert werden soll.
`–getloglevel`	Zeigt die aktuelle Protokollierungsebene von View Agent an.
`–getstatus`	Zeigt den Status von View Agent an.
`–getversion`	Zeigt die Version von View Agent an.
`–list`	Zeigt eine Liste der Protokolldateien für View Agent an.
`–m` *Maschine*	Gibt die Maschine innerhalb eines Desktop-Pools an.
`–outfile` *lokale_Datei*	Gibt den Namen der lokalen Datei an, in der ein DCT-Paket oder die Kopie einer Protokolldatei gespeichert werden soll.
`–setloglevel` *Ebene*	Legt die Protokollierungsebene von View Agent fest. **debug** – Protokolliert Fehler-, Warnungs- und Debugging-Ereignisse. **normal** – Protokolliert Fehler- und Warnungsereignisse. **trace** – Protokolliert Fehler-, Informations- und Debugging-Ereignisse.

Beispiele

Zeigen Sie die Agent-Protokollierungsebene für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** an.

```
vdmadmin –A –d dtpool2 –m machine1 –getloglevel
```

Legen Sie die View Agent-Protokollierungsebene für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** auf **[Debug]** fest.

```
vdmadmin –A –d dtpool2 –m machine1 –setloglevel debug
```

Zeigen Sie die Liste der View Agent-Protokolldateien für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** an.

```
vdmadmin –A –d dtpool2 –m machine1 –list
```

Speichern Sie eine Kopie der View Agent-Protokolldatei `log–2009–01–02.txt` für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** als `C:\mycopiedlog.txt`.

```
vdmadmin –A –d dtpool2 –m machine1 –getlogfile log–2009–01–02.txt –outfile C:\mycopiedlog.txt
```

Zeigen Sie die Version der View Agent-Instanz für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** an.

```
vdmadmin –A –d dtpool2 –m machine1 –getversion
```

Zeigen Sie den Status der View Agent-Instanz für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** an.

```
vdmadmin –A –d dtpool2 –m machine1 –getstatus
```

Erstellen Sie das DCT-Paket für die Maschine **[machine1]** im Desktop-Pool **[dtpool2]** und schreiben Sie es in die .zip-Datei `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Außerkraftsetzen von IP-Adressen unter Verwendung der Option „-A“

Sie können den Befehl `vdmadmin` mit der Option `–A` verwenden, um die von einer View Agent-Instanz angegebene IP-Adresse außer Kraft zu setzen.

Syntax

```
vdmadmin –A [–b Authentifizierungsargumente] –override –i IP_oder_DNS –d Desktop –m Maschine

vdmadmin –A [–b Authentifizierungsargumente] –override –list –d Desktop –m Maschine

vdmadmin –A [–b Authentifizierungsargumente] –override –r –d Desktop [–m Maschine]
```

Nutzungshinweise

Eine View Agent-Instanz gibt die ermittelte IP-Adresse der Maschine, auf der sie ausgeführt wird, an die View Connection Server-Instanz zurück. In Konfigurationen, in denen die View Connection Server-Instanz den von der View Agent-Instanz bereitgestellten Wert nicht als vertrauenswürdig einstuft, können Sie diesen Wert außer Kraft setzen und die IP-Adresse festlegen, welche die verwaltete Maschine verwenden sollte. Wenn die von der View Agent-Instanz angegebene Adresse einer Maschine nicht mit der definierten Adresse übereinstimmt, kann nicht über eine View Client-Instanz auf die Maschine zugegriffen werden.

Options (Optionen)

Tabelle 17-4 zeigt die verfügbaren Optionen zum Außerkraftsetzen von IP-Adressen.

Tabelle 17-4. Optionen für das Außerkraftsetzen von IP-Adressen

Option	Beschreibung
`–d` *Desktop*	Gibt den Desktop-Pool an.
`–i` *IP_oder_DNS*	Gibt die IP-Adresse oder den auflösbaren Domänennamen in DNS an.
`–m` *Maschine*	Gibt den Namen der Maschine in einem Desktop-Pool an.
`–override`	Gibt einen Vorgang zum Außerkraftsetzen von IP-Adressen an.
`–r`	Entfernt eine außer Kraft gesetzte IP-Adresse.

Beispiele

Setzen Sie die IP-Adresse für die Maschine **[machine2]** im Desktop-Pool **[dtpool2]** außer Kraft.

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

Zeigen Sie die IP-Adressen an, die für die Maschine **[machine2]** im Desktop-Pool **[dtpool2]** definiert wurden.

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

Entfernen Sie die IP-Adressen, die für die Maschine **[machine2]** im Desktop-Pool **[dtpool2]** definiert wurden.

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

Entfernen Sie die IP-Adressen, die für die Desktops im Desktop-Pool **[dtpool3]** definiert wurden.

```
vdmadmin –A –override –r –d dtpool3
```

Festlegen des Namens einer View Connection Server-Gruppe unter Verwendung der Option „-C“

Sie können den Befehl `vdmadmin` mit der Option `–C` verwenden, um den Namen einer View Connection Server-Gruppe festzulegen. Zur Identifizierung der Gruppe in Microsoft System Center Operations Manager (SCOM) wird dieser Name in der SCOM-Konsole angezeigt.

Syntax

`vdmadmin –C [–b` *`Authentifizierungsargumente`*`] [–c` *`Gruppenname`*`]`

Nutzungshinweise

Wenn zur Überwachung und Verwaltung von View Manager-Komponenten SCOM verwendet werden soll, muss eine View Connection Server-Gruppe benannt werden. In View Administrator wird der Name einer Gruppe nicht angezeigt. Führen Sie den Befehl auf einem Mitglied der Gruppe aus, der Sie einen Namen zuweisen möchten.

Wenn Sie keinen Namen für die Gruppe angeben, gibt der Befehl die GUID der Gruppe zurück, zu der die lokale View Connection Server-Instanz gehört. Anhand der GUID können Sie überprüfen, ob eine View Connection Server-Instanz Mitglied derselben View Connection Server-Gruppe ist wie eine andere View Connection Server-Instanz.

Die Verwendung von SCOM mit VMware View ist im Dokument *Integration von VMware View* beschrieben.

Options (Optionen)

Die Option `–c` gibt den Namen der View Connection Server-Gruppe an. Wenn Sie diese Option nicht angeben, gibt der Befehl die GUID der Gruppe zurück.

Beispiele

Legen Sie den Namen einer View Connection Server-Gruppe auf **[VCSG01]** fest.

```
vdmadmin –C –c VCSG01
```

Geben Sie die GUID der Gruppe zurück.

```
vdmadmin –C
```

Aktualisieren der fremden Sicherheitsprinzipale unter Verwendung der Option „-F“

Mithilfe des Befehls `vdmadmin` können über die Option `–F` die fremden Sicherheitsprinzipale (Foreign Security Principals, FSPs) von Windows-Benutzern in Active Directory aktualisiert werden, die für die Verwendung eines Desktops berechtigt sind.

Syntax

`vdmadmin –F [–b` *`Authentifizierungsargumente`*`] [–u` *`Domäne\Benutzer`*`]`

Nutzungshinweise

Wenn Sie Domänen außerhalb Ihrer lokalen Domänen als vertrauenswürdig einstufen, lassen Sie den Zugriff auf die Ressourcen der lokalen Domänen durch Sicherheitsprinzipale in den externen Domänen zu. In Active Directory werden Sicherheitsprinzipale in vertrauenswürdigen externen Domänen durch fremde Sicherheitsprinzipale repräsentiert. Wenn Sie die Liste der vertrauenswürdigen externen Domänen ändern, kann die Aktualisierung der fremden Sicherheitsprinzipale erforderlich sein.

Options (Optionen)

Die Option –u gibt den Namen und die Domäne des Benutzers an, dessen FSP aktualisiert werden soll. Wenn Sie diese Option nicht festlegen, werden über den Befehl die FSPs aller Benutzer in Active Directory aktualisiert.

Beispiele

Aktualisieren Sie den fremden Sicherheitsprinzipal des Benutzers **[Jim]** in der Domäne **[EXTERNAL]** .

```
vdmadmin –F –u EXTERNAL\Jim
```

Aktualisieren Sie die fremden Sicherheitsprinzipale aller Benutzer in Active Directory.

```
vdmadmin –F
```

Auflisten und Anzeigen von Systemüberwachungen unter Verwendung der Option „-H“

Mithilfe der Option –H des Befehls vdmadmin können die vorhandenen Systemüberwachungen angezeigt werden, um Instanzen für View Manager-Komponenten zu überwachen und die Einzelheiten für eine bestimmte Systemüberwachung oder eine bestimmte Überwachungsinstanz anzuzeigen.

Syntax

```
vdmadmin –H [–b Authentifizierungsargumente] –list –xml [–w | –n]
```

```
vdmadmin –H [–b Authentifizierungsargumente] –list –monitorid Monitor–ID –xml [–w | –n]
```

```
vdmadmin –H [–b Authentifizierungsargumente] –monitorid Monitor–ID –instanceid Istanzen–ID –xml
[–w | –n]
```

Nutzungshinweise

Tabelle 17-5 zeigt die von View Manager verwendeten Systemüberwachungen, um den Zustand der Komponenten zu überwachen.

Tabelle 17-5. Systemüberwachungen

Überwachungsinstanz	Beschreibung
CBMonitor	Überwacht den Zustand von View Connection Server-Instanzen.
DBMonitor	Überwacht den Zustand der Ereignisdatenbank.
DomainMonitor	Überwacht den Zustand der lokalen Domäne und aller vertrauenswürdigen Domänen des View Connection Server-Hosts.
SGMonitor	Überwacht den Zustand von Sicherheits-Gateway-Diensten und Sicherheitsservern.

Tabelle 17-5. Systemüberwachungen (Fortsetzung)

Überwachungsinstanz	Beschreibung
TSMonitor	Überwacht den Zustand von Übertragungsservern.
VCMonitor	Überwacht den Zustand von vCenter Server-Instanzen.

Wenn eine Komponente über mehrere Instanzen verfügt, erstellt View Manager eine separate Überwachungsinstanz für die Überwachung jeder einzelnen Komponenteninstanz.

Der Befehl gibt sämtliche Informationen zu Systemüberwachungen und Überwachungsinstanzen im XML-Format aus.

Options (Optionen)

Tabelle 17-6 zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Systemüberwachungen.

Tabelle 17-6. Optionen für das Auflisten und Anzeigen von Systemüberwachungen

Option	Beschreibung
`–instanceid` *Instanzen-ID*	Gibt eine Systemüberwachungsinstanz an.
`–list`	Zeigt die vorhandenen Systemüberwachungen an, wenn keine Systemüberwachungs-ID angegeben wird.
`–list –monitorid` *Monitor-ID*	Zeigt die Überwachungsinstanzen für die angegebene Systemüberwachungs-ID an.
`–monitorid` *Monitor-ID*	Gibt eine Systemüberwachungs-ID an.

Beispiele

Listen Sie alle vorhandenen Systemüberwachungen im XML-Format mit Unicode-Zeichen auf.

```
vdmadmin –H –list –xml
```

Listen Sie alle Instanzen der vCenter-Überwachung (VCMonitor) im XML-Format mit ASCII-Zeichen auf.

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

Zeigen Sie den Zustand einer angegebenen vCenter-Überwachungsinstanz an.

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

Auflisten und Anzeigen von Berichten zum View Manager-Betrieb unter Verwendung der Option „-I“

Sie können den Befehl `vdmadmin` mit der Option `–I` verwenden, um die verfügbaren Berichte zum View Manager-Betrieb aufzulisten und die Ergebnisse beim Ausführen eines dieser Berichte anzuzeigen.

Syntax

```
vdmadmin –I [–b Authentifizierungsargumente] –list [–xml] [–w | –n]
```

```
vdmadmin –I [–b Authentifizierungsargumente] –report Bericht –view Ansicht [–startdate JJJJ–MM–TT–HH:mm:ss][–enddate JJJJ–MM–TT–HH:mm:ss] [–w | –n] –xml | –csv
```

Nutzungshinweise

Sie können den Befehl zum Anzeigen der verfügbaren Berichte und Ansichten sowie zum Anzeigen der Informationen verwenden, die View Manager für einen angegebenen Bericht oder eine angegebene Ansicht aufgezeichnet hat.

Options (Optionen)

Tabelle 17-7 zeigt die verfügbaren Optionen zum Auflisten und Anzeigen von Berichten und Ansichten.

Tabelle 17-7. Optionen für das Auflisten und Anzeigen von Berichten und Ansichten

Option	Beschreibung
`–enddate` *JJJJ-MM-TT-HH:mm:ss*	Gibt das Enddatum des Zeitraums an, für den Informationen angezeigt werden sollen.
`–list`	Zeigt eine Liste der verfügbaren Berichte und Ansichten an.
`–report` *Bericht*	Gibt einen Bericht an.
`–startdate` *JJJJ-MM-TT-HH:mm:ss*	Gibt das Startdatum des Zeitraums an, für den Informationen angezeigt werden sollen.
`–view` *Ansicht*	Gibt eine Ansicht an.

Beispiele

Listen Sie die verfügbaren Berichte und Ansichten im XML-Format mit Unicode-Zeichen auf.

```
vdmadmin –I –list –xml –w
```

Zeigen Sie eine Liste der Benutzerereignisse seit dem 1. August 2010 im CSV-Format mit ASCII-Zeichen an.

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

Zuweisen von dedizierten Desktops unter Verwendung der Option „-L“

Mithilfe des Befehls `vdmadmin` können Sie über die Option –L Benutzern Desktops aus einem dedizierten Pool zuweisen.

Syntax

```
vdmadmin –L [–b Authentifizierungsargumente] –d Desktop –m  Maschine –u Domäne\Benutzer
```

```
vdmadmin –L [–b Authentifizierungsargumente] –d Desktop –m  Maschine | –u Domäne\Benutzer] –r
```

Nutzungshinweise

View Manager weist Benutzern Desktops zu, wenn sich diese zum ersten Mal mit einem dedizierten Desktop-Pool verbinden. Unter bestimmten Umständen kann es sinnvoll sein, Benutzern Desktops bereits vorab zuzuweisen. Zum Beispiel sollen die Systemumgebungen möglicherweise vorbereitet werden, bevor die Benutzer erstmalig eine Verbindung herstellen. Nachdem ein Benutzer eine Verbindung mit einem Desktop herstellt, der von View Manager aus einem dedizierten Pool zugewiesen wird, bleibt dieser Desktop während der gesamten Lebensdauer der Desktop-Quelle diesem Benutzer zugewiesen. Sie können einen Benutzer einer einzelnen virtuellen Maschine in einem dedizierten Pool zuweisen.

Sie können einen Desktop einem beliebigen berechtigten Benutzer zuweisen. Dies kann notwendig sein, wenn Sie nach dem Verlust von View LDAP-Daten auf einer View Connection Server-Instanz eine Wiederherstellung durchführen oder wenn Sie den Besitz einer bestimmten Desktop-Quelle ändern möchten.

Nachdem ein Benutzer eine Verbindung mit einem Desktop herstellt, der von View Manager aus einem dedizierten Pool zugewiesen wird, bleibt dieser Desktop während der gesamten Lebensdauer der Desktop-Quelle diesem Benutzer zugewiesen. Möglicherweise möchten Sie die Zuweisung eines Desktops zu einem Benutzer entfernen, wenn ein Benutzer nicht mehr für die Organisation tätig ist, nicht länger auf den Desktop zugreifen muss oder einen Desktop in einem anderen Desktop-Pool verwenden wird. Es ist auch möglich, die Zuweisungen für sämtliche Benutzer zu entfernen, die auf einen Desktop-Pool zugreifen.

Optionen

Tabelle 17-8 zeigt die Optionen an, die Sie für die Zuweisung eines Benutzers zu einem Desktop oder zum Entfernen einer Zuweisung festlegen können.

Tabelle 17-8. Optionen für die Zuweisung dedizierter Desktops

Option	Beschreibung
`–d` *Desktop*	Legt den Namen des Desktop-Pools fest.
`–m` *Maschine*	Legt den Namen der virtuellen Maschine fest.
`–r`	Entfernt eine Zuweisung für einen bestimmten Benutzer oder entfernt die gesamten Zuweisungen für eine bestimmte Maschine.
`–u` *Domäne\Benutzer*	Legt den Anmeldenamen und die Domäne des Benutzers fest.

Beispiele

Weisen Sie die Maschine **[machine2]** im Desktop-Pool **[dtpool1]** dem Benutzer **[Jo]** in der Domäne **[CORP]** zu.

```
vdmadmin –L –d dtpool1 –m machine2 –u CORP\Jo
```

Entfernen Sie die Zuweisungen für den Benutzer **[Jo]** in der Domäne **[CORP]** für Desktops im Pool **[dtpool1]** .

```
vdmadmin –L –d dtpool1 –u Corp\Jo –r
```

Entfernen Sie sämtliche Benutzerzuweisungen für die Maschine **[machine1]** im Desktop-Pool **[dtpool3]** .

```
vdmadmin –L –d dtpool3 –m machine1 –r
```

Anzeigen von Informationen zu Maschinen unter Verwendung der Option „-M“

Sie können den Befehl `vdmadmin` mit der Option `–M` verwenden, um Informationen zur Konfiguration virtueller Maschinen oder physischer Computer anzuzeigen.

Syntax

```
vdmadmin –M [–b Authentifizierungsargumente] [–m Maschine | [[–u Domäne\Benutzer][–d Desktop]]
[–xml | –csv] [–w | –n]
```

Nutzungshinweise

Dieser Befehl zeigt Informationen zur zugrunde liegenden virtuellen Maschine oder zum zugrunde liegenden physischen Computer eines Desktops an.

- Anzeigename der Maschine.
- Name des Desktop-Pools.

- Status der Maschine.
- SID des zugewiesenen Benutzers.
- Kontoname des zugewiesenen Benutzers.
- Domänenname des zugewiesenen Benutzers.
- Offline-Status eines lokalen Desktops (gilt nicht für Version 4.0 oder früher).
- Gegebenenfalls der Bestandslistenpfad der virtuellen Maschine.
- Erstellungsdatum der Maschine.
- Gegebenenfalls der Vorlagenpfad der Maschine.
- Gegebenenfalls die vCenter Server-URL.

Options (Optionen)

Tabelle 17-9 zeigt die verfügbaren Optionen zum Angeben der Maschine, für die Details angezeigt werden sollen.

Tabelle 17-9. Optionen für das Anzeigen von Informationen zu Maschinen

Option	Beschreibung
`–d` *Desktop*	Legt den Namen des Desktop-Pools fest.
`–m` *Maschine*	Legt den Namen der virtuellen Maschine fest.
`–u` *Domäne\Benutzer*	Legt den Anmeldenamen und die Domäne des Benutzers fest.

Beispiele

Zeigen Sie Informationen zur zugrunde liegenden Maschine für den Desktop im Pool **[dtpool2]** an, der dem Benutzer **[Jo]** in der Domäne **[CORP]** zugewiesen ist, und legen Sie für die Ausgabe das XML-Format mit ASCII-Zeichen fest.

```
vdmadmin –M –u CORP\Jo –d dtpool2 –xml –n
```

Zeigen Sie Informationen zur Maschine **[machine3]** an und legen Sie für die Ausgabe das CSV-Format fest.

```
vdmadmin –M –m machine3 –csv
```

Konfigurieren von Domänenfiltern unter Verwendung der Option „-N“

Sie können den Befehl `vdmadmin` mit der Option `–N` zum Steuern der Domänen verwenden, die View Manager für die Endbenutzer zur Verfügung stellt.

Syntax

```
vdmadmin –N [–b Authentifizierungsargumente] –domains {–exclude | –include | –search} –domain Domäne –add [–s Verbindungsserver]
```

```
vdmadmin –N [–b Authentifizierungsargumente] –domains –list [–w | –n] [–xml]
```

```
vdmadmin –N [–b Authentifizierungsargumente] –domains –list –active [–w | –n] [–xml]
```

```
vdmadmin –N [–b Authentifizierungsargumente] –domains {–exclude | –include | –search} –domain Domäne –remove [–s Verbindungsserver]
```

```
vdmadmin –N [–b Authentifizierungsargumente] –domains {–exclude | –include | –search} –removeall [–s Verbindungsserver]
```

Nutzungshinweise

Geben Sie die Option `–exclude`, `–include` oder `–search` an, um einen Vorgang auf die Ausschlussliste, die Aufnahmeliste oder die Ausschlussliste für die Suche anzuwenden.

Wenn Sie eine Domäne zu einer Ausschlussliste für die Suche hinzufügen, wird die Domäne bei einer automatisierten Domänensuche ausgeschlossen.

Beim Hinzufügen einer Domäne zu einer Aufnahmeliste wird die Domäne in die Ergebnisse der Suche aufgenommen.

Wenn Sie eine Domäne zu einer Ausschlussliste hinzufügen, wird die Domäne aus den Ergebnissen der Suche ausgeschlossen.

Optionen

Tabelle 17-10 zeigt die verfügbaren Optionen zum Konfigurieren von Domänenfiltern.

Tabelle 17-10. Optionen für die Konfiguration von Domänenfiltern

Option	Beschreibung
`–add`	Fügt eine Domäne zu einer Liste hinzu.
`–domain` *Domäne*	Gibt die Domäne für die Filterung an. Verwenden Sie zum Angeben von Domänen nicht den DNS-Namen, sondern den NetBIOS-Namen.
`–domains`	Gibt einen Domänenfiltervorgang an.
`–exclude`	Gibt einen Vorgang für eine Ausschlussliste an.
`–include`	Gibt einen Vorgang für eine Aufnahmeliste an.
`–list`	Zeigt die Domänen an, die in der Ausschlussliste für die Suche, in der Ausschlussliste und in der Aufnahmeliste für die einzelnen View Connection Server-Instanzen und für die View Connection Server-Gruppe konfiguriert sind.
`–list –active`	Zeigt die verfügbaren Domänen für die View Connection Server-Instanz an, auf welcher der Befehl ausgeführt wird.
`–remove`	Entfernt eine Domäne aus einer Liste.
`–removeall`	Entfernt alle Domänen aus einer Liste.
`–s` *Verbindungsserver*	Gibt an, dass der Vorgang für die Domänenfilter einer View Connection Server-Instanz ausgeführt wird. Die View Connection Server-Instanz kann über den Namen oder die IP-Adresse angegeben werden. Wenn Sie diese Option nicht angeben, werden Änderungen an der Suchkonfiguration für alle View Connection Server-Instanzen innerhalb der Gruppe übernommen.
`–search`	Gibt einen Vorgang für eine Ausschlussliste für die Suche an.

Beispiele

Fügen Sie die Domäne **[FARDOM]** zur Ausschlussliste für die Suche für die View Connection Server-Instanz **[csvr1]** hinzu.

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

Fügen Sie die Domäne **[NEARDOM]** zur Ausschlussliste für eine View Connection Server-Gruppe hinzu.

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

Zeigen Sie die Konfiguration für die Domänensuche auf beiden View Connection Server-Instanzen in der Gruppe und für die Gruppe an.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

View Manager schränkt die Domänensuche auf allen View Connection Server-Hosts in der Gruppe ein, indem die Domänen **[FARDOM]** und **[DEPTX]** ausgeschlossen werden. Die Zeichen (*) neben der Ausschlussliste für **[CONSVR-1]** zeigen an, dass View Manager die Domäne **[YOURDOM]** aus den Ergebnissen der Domänensuche auf **[CONSVR-1]** ausschließt.

Zeigen Sie die Domänenfilter im XML-Format mit ASCII-Zeichen an.

```
vdmadmin –N –domains –list –xml –n
```

Zeigen Sie die Domänen an, die für View Manager auf der lokalen View Connection Server-Instanz verfügbar sind.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : FARDOM DNS:fardom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
Domain            : DEPTY DNS:depty.mycorp.com
Domain            : DEPTZ DNS:deptz.mycorp.com
```

Zeigen Sie die verfügbaren Domänen im XML-Format mit ASCII-Zeichen an.

```
vdmadmin –N –domains –list –active –xml –n
```

Entfernen Sie die Domäne **[NEARDOM]** aus der Ausschlussliste für eine View Connection Server-Gruppe.

```
vdmadmin –N –domains –exclude –domain NEARDOM –remove
```

Entfernen Sie sämtliche Domänen aus der Aufnahmeliste für die View Connection Server-Instanz **[csvr1]** .

```
vdmadmin –N –domains –include –removeall –s csvr1
```

Konfigurieren von Domänenfiltern

Domänenfilter können Sie zur Einschränkung der Anzahl der Domänen, die eine View Connection Server-Instanz oder ein Sicherheitsserver den Endbenutzern zur Verfügung stellt, konfigurieren.

View Manager ermittelt die für den Zugriff verfügbaren Domänen, indem – beginnend mit der Domäne, in der sich eine View Connection Server-Instanz oder ein Sicherheitsserver befindet – die vorhandenen Vertrauensbeziehungen durchlaufen werden. Bei einer kleinen, gut verbundenen Gruppe von Domänen kann View Manager schnell eine vollständige Liste der vorhandenen Domänen erstellen. Liegt jedoch eine große Anzahl an Domänen oder eine weniger gute Verbindung zwischen den Domänen vor, steigt der zur Ermittlung der Domänen benötigte Zeitaufwand. Die View Manager-Suchergebnisse können Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sich diese mit ihren Desktops verbinden.

Wenn Sie den Wert des Windows-Registrierungsschlüssels zum Steuern der rekursiven Domänenenumeration (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) zuvor auf **[false]** gesetzt haben, ist die rekursive Domänensuche deaktiviert und die View Connection Server-Instanz verwendet nur die primäre Domäne. Löschen Sie zum Verwenden der Domänenfilterungsfunktion den Registrierungsschlüssel oder setzen Sie seinen Wert auf **[true]** . Starten Sie das System anschließend neu. Dieser Schritt muss für jede View Connection Server-Instanz ausgeführt werden, auf der dieser Schlüssel festgelegt ist.

Tabelle 17-11 zeigt die Typen von Domänenlisten, die Sie zur Konfiguration der Domänenfilterung angeben können.

Tabelle 17-11. Typen von Domänenlisten

Domänenlistentyp	Beschreibung
Ausschlussliste für die Suche	Gibt die Domänen an, die View Manager während einer automatisierten Suche durchlaufen kann. Bei der Suche werden Domänen ignoriert, die in der Ausschlussliste für die Suche enthalten sind. Es wird nicht versucht, Domänen zu ermitteln, denen die ausgeschlossenen Domänen vertrauen. Die primäre Domäne kann nicht aus der Suche ausgeschlossen werden.
Ausschlussliste	Gibt die Domänen an, die View Manager aus den Ergebnissen einer Domänensuche ausschließt. Die primäre Domäne kann nicht ausgeschlossen werden.
Aufnahmeliste	Gibt die Domänen an, die View Manager nicht aus den Ergebnissen einer Domänensuche ausschließt. Mit Ausnahme der primären Domäne werden alle anderen Domänen entfernt.

Bei der automatisierten Domänensuche wird eine Liste mit Domänen abgerufen. Dabei werden die in der Ausschlussliste für die Suche angegebenen Domänen sowie Domänen, denen diese ausgeschlossenen Domänen vertrauen, ausgeschlossen. View Manager wählt die erste nicht leere Ausschluss- oder Aufnahmeliste mit dieser Reihenfolge.

1 Die für die View Connection Server-Instanz konfigurierte Ausschlussliste.

2 Die für die View Connection Server-Gruppe konfigurierte Ausschlussliste.

3 Die für die View Connection Server-Instanz konfigurierte Aufnahmeliste.

4 Die für die View Connection Server-Gruppe konfigurierte Aufnahmeliste.

View Manager wendet lediglich die erste ausgewählte Liste auf die Suchergebnisse an.

Wenn Sie eine Domäne in die Aufnahmeliste aufnehmen, deren Domänencontroller nicht verfügbar ist, nimmt View Manager diese Domäne nicht in die Liste aktiver Domänen auf.

Die primäre Domäne, zu der eine View Connection Server-Instanz oder ein Sicherheitsserver gehört, kann nicht ausgeschlossen werden.

Beispiel für die Filterung zum Einschließen von Domänen

Sie können mithilfe einer Aufnahmeliste Domänen angeben, die View Manager nicht aus den Ergebnissen einer Domänensuche ausschließt. Mit Ausnahme der primären Domäne werden alle anderen Domänen entfernt.

Eine View Connection Server-Instanz ist mit der primären Domäne **[MYDOM]** verbunden und verfügt über eine Vertrauensbeziehung mit der Domäne **[YOURDOM]** . Die Domäne **[YOURDOM]** verfügt über eine Vertrauensbeziehung mit der Domäne **[DEPTX]** .

Zeigen Sie die derzeit aktiven Domänen für die View Connection Server-Instanz an.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : FARDOM DNS: fardom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
Domain            : DEPTY DNS:depty.mycorp.com
Domain            : DEPTZ DNS:deptz.mycorp.com
```

Die Domänen **[DEPTY]** und **[DEPTZ]** sind in der Liste enthalten, da sie vertrauenswürdige Domänen der Domäne **[DEPTX]** sind.

Geben Sie an, dass die View Connection Server-Instanz neben der primären Domäne **[MYDOM]** nur die Domänen **[YOURDOM]** und **[DEPTX]** verfügbar machen soll.

```
vdmadmin –N –domains –include –domain YOURDOM –add
vdmadmin –N –domains –include –domain DEPTX –add
```

Zeigen Sie die derzeit aktiven Domänen an, nachdem die Domänen **[YOURDOM]** und **[DEPTX]** aufgenommen wurden.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
```

View Manager wendet die Aufnahmeliste auf die Ergebnisse einer Domänensuche an. Wenn die Domänenhierarchie sehr komplex ist oder die Netzwerkverbindungen zu einigen Domänen eine geringe Leistung bieten, wird die Domänensuche möglicherweise langsam ausgeführt. Verwenden Sie in diesen Fällen stattdessen die Ausschlussliste für die Suche.

Beispiel für die Filterung zum Ausschließen von Domänen

Sie können mithilfe einer Aufnahmeliste Domänen angeben, die View Manager aus den Ergebnissen einer Domänensuche ausschließt.

Eine Gruppe aus zwei View Connection Server-Instanzen, **[CONSVR-1]** und **[CONSVR-2]** , ist mit der primären Domäne **[MYDOM]** verbunden und verfügt über eine Vertrauensbeziehung mit der Domäne **[YOURDOM]** . Die Domäne **[YOURDOM]** verfügt über eine Vertrauensbeziehung mit den Domänen **[DEPTX]** und **[FARDOM]** .

Die Domäne **[FARDOM]** befindet sich an einem geografisch entfernten Standort und die Netzwerkkonnektivität mit dieser Domäne wird über eine langsame Verbindung mit hoher Latenz hergestellt. Benutzer in der Domäne **[FARDOM]** müssen nicht auf die View Connection Server-Gruppe in der Domäne **[MYDOM]** zugreifen können.

Zeigen Sie die derzeit aktiven Domänen für ein Mitglied der View Connection Server-Gruppe an.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : FARDOM DNS: fardom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
Domain            : DEPTY DNS:depty.mycorp.com
Domain            : DEPTZ DNS:deptz.mycorp.com
```

Bei den Domänen **[DEPTY]** und **[DEPTZ]** handelt es sich um vertrauenswürdige Domänen der Domäne **[DEPTX]** .

Zum Verbessern der Verbindungsleistung für View Client-Instanzen schließen Sie die Domäne **[FARDOM]** aus der Suche der View Connection Server-Gruppe aus.

```
vdmadmin –N –domains –search –domain FARDOM –add
```

Der Befehl zeigt die derzeit aktiven Domänen an, nachdem die Domäne **[FARDOM]** aus der Suche ausgeschlossen wurde.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
Domain            : DEPTX DNS:deptx.mycorp.com
Domain            : DEPTY DNS:depty.mycorp.com
Domain            : DEPTZ DNS:deptz.mycorp.com
```

Erweitern Sie die Ausschlussliste für die Suche, um die Domäne **[DEPTX]** sowie all ihre als vertrauenswürdig eingestuften Domänen aus der Domänensuche für alle View Connection Server-Instanzen einer Gruppe auszuschließen. Schließen Sie zudem die Domäne **[YOURDOM]** aus den verfügbaren Domänen auf **[CONSVR-1]** aus.

```
vdmadmin –N –domains –search –domain DEPTX –add
vdmadmin –N –domains –exclude –domain YOURDOM –add –s CONSVR–1
```

Zeigen Sie die neue Konfiguration für die Domänensuche an.

```
C:\ vdmadmin -N -domains -list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR-1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR-2
   Include:
   Exclude:
   Search :
```

View Manager schränkt die Domänensuche auf allen View Connection Server-Hosts in der Gruppe ein, indem die Domänen **[FARDOM]** und **[DEPTX]** ausgeschlossen werden. Die Zeichen (*) neben der Ausschlussliste für **[CONSVR-1]** zeigen an, dass View Manager die Domäne **[YOURDOM]** aus den Ergebnissen der Domänensuche auf **[CONSVR-1]** ausschließt.

Zeigen Sie auf **[CONSVR-1]** die derzeit aktiven Domänen an.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=============================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
```

Zeigen Sie auf **[CONSVR-2]** die derzeit aktiven Domänen an.

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=============================
Primary Domain: MYDOM

Domain            : MYDOM DNS:mydom.mycorp.com
Domain            : YOURDOM DNS:yourdom.mycorp.com
```

Anzeigen der Desktops und Richtlinien für nicht berechtigte Benutzer unter Verwendung der Optionen „-O“ und „-P“

Sie können den Befehl `vdmadmin` mit den Optionen `–O` und `–P` verwenden, um die Desktops und Richtlinien von Benutzern anzuzeigen, die nicht länger für die Verwendung des Systems berechtigt sind.

Syntax

```
vdmadmin –O [–b Authentifizierungsargumente] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath Pfad]]
```

```
vdmadmin –P [–b Authentifizierungsargumente] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath Pfad]]
```

Nutzungshinweise

Wenn Sie die Berechtigungen eines Benutzers für einen persistenten Desktop oder ein physisches System aufheben, wird die verknüpfte Desktop-Zuweisung nicht automatisch entfernt. Dies kann akzeptabel sein, wenn ein Benutzerkonto temporär gesperrt wird oder sich der Benutzer in einem Sabbatjahr befindet. Bei erneuter Aktivierung der Berechtigung kann der Benutzer denselben Desktop wie zuvor weiterverwenden. Wenn ein Benutzer nicht mehr in der Organisation beschäftigt ist, können andere Benutzer nicht auf den Desktop zugreifen und der Desktop wird als verwaist betrachtet. Zudem sollten die Richtlinien geprüft werden, die nicht berechtigten Benutzern zugewiesen sind.

Options (Optionen)

Tabelle 17-12 zeigt die verfügbaren Optionen zum Anzeigen der Desktops und Richtlinien nicht berechtigter Benutzer.

Tabelle 17-12. Optionen für das Anzeigen der Desktops und Richtlinien nicht berechtigter Benutzer

Option	Beschreibung
`–ld`	Sortiert die Einträge der Ausgabe nach Desktop.
`–lu`	Sortiert die Einträge der Ausgabe nach Benutzer.
`–noxslt`	Gibt an, dass das standardmäßige Stylesheet nicht auf die XML-Ausgabe angewendet wird.
`–xsltpath` *Pfad*	Gibt den Pfad zum Stylesheet an, das zur Umwandlung der XML-Ausgabe verwendet wird.

Tabelle 17-13 zeigt die verfügbaren Stylesheets, um die XML-Ausgabe in das HTML-Format umzuwandeln. Die Stylesheets befinden sich im Verzeichnis `C:\Programme\VMware\VMware View\server\etc`.

Tabelle 17-13. XSL-Stylesheets

Name der Stylesheet-Datei	Beschreibung
`list–checkedout–unentitled.xsl`	Zur Umwandlung von Berichten mit einer Liste der Desktops, die von nicht berechtigten Benutzern ausgecheckt wurden.
`unentitled–machines.xsl`	Zur Umwandlung von Berichten mit einer Liste nicht berechtigter Desktops, die nach Benutzer oder nach System gruppiert und derzeit einem Benutzer zugewiesen sind. Dies ist das standardmäßige Stylesheet.
`unentitled–policies.xsl`	Zur Umwandlung von Berichten mit einer Liste von Desktops, denen Richtlinien auf Benutzerebene zugewiesen sind, die auf nicht berechtigte Benutzer angewendet werden.

Beispiele

Zeigen Sie die nicht berechtigten Benutzern zugewiesenen Desktops an und legen Sie eine Gruppierung nach Desktop sowie die Ausgabe im Textformat fest.

```
vdmadmin –O –ld
```

Zeigen Sie die nicht berechtigten Benutzern zugewiesenen Desktops an und legen Sie eine Gruppierung nach Benutzer sowie die Ausgabe im XML-Format mit ASCII-Zeichen fest.

```
vdmadmin –O –lu –xml –n
```

Wenden Sie Ihr eigenes Stylesheet `C:\tmp\unentitled–users.xsl` an und legen Sie die Speicherung der Ausgabe in der Datei `uu–output.html` fest.

```
vdmadmin –O –lu –xml –xsltpath "C:\tmp\unentitled–users.xsl" > uu–output.html
```

Zeigen Sie die Benutzerrichtlinien an, die den Desktops nicht berechtigter Benutzer zugewiesen sind, und legen Sie eine Gruppierung nach Desktop sowie die Ausgabe im XML-Format mit Unicode-Zeichen fest.

```
vdmadmin –P –ld –xml –w
```

Wenden Sie Ihr eigenes Stylesheet `C:\tmp\unentitled–policies.xsl` an und legen Sie die Speicherung der Ausgabe in der Datei `up–output.html` fest.

```
vdmadmin –P –ld –xml –xsltpath "C:\tmp\unentitled–policies.xsl" > up–output.html
```

Konfigurieren von Clients im Kiosk-Modus unter Verwendung der Option „-Q“

Unter Verwendung des Befehls `vdmadmin` mit der Option `–Q` können Standardwerte festgelegt und Konten für Clients im Kiosk-Modus erstellt werden, um die Authentifizierung für diese Clients zu aktivieren und Informationen zu ihrer Konfiguration anzuzeigen.

Syntax

vdmadmin –Q –clientauth –add [–b *Authentifizierungsargumente*] –domain *Domänenname*–clientid *Client–ID* [–password "*Kennwort*" | –genpassword] [–ou *DN*] [–expirepassword | –noexpirepassword] [–group *Gruppenname* | –nogroup] [–description "*Beschreibung*"]

vdmadmin –Q –disable [–b *Authentifizierungsargumente*] –s *Verbindungsserver*

vdmadmin –Q –enable [–b *Authentifizierungsargumente*] –s *Verbindungsserver* [–requirepassword]

vdmadmin –Q –clientauth –getdefaults [–b *Authentifizierungsargumente*] [–xml]

vdmadmin –Q –clientauth –list [–b *Authentifizierungsargumente*] [–xml]

vdmadmin –Q –clientauth –remove [–b *Authentifizierungsargumente*] –domain *Domänenname*–clientid *Client–ID*

vdmadmin –Q –clientauth –removeall [–b *Authentifizierungsargumente*] [–force]

vdmadmin –Q –clientauth –setdefaults [–b *Authentifizierungsargumente*] [–ou *DN*] [–expirepassword | –noexpirepassword] [–group *Gruppenname* | –nogroup]

vdmadmin –Q –clientauth –update [–b *Authentifizierungsargumente*] –domain *Domänenname*–clientid *Client–ID* [–password "*Kennwort*" | –genpassword] [–description "*Beschreibungstext*"]

Nutzungshinweise

Der Befehl `vdmadmin` muss für eine der View Connection Server-Instanzen in der Gruppe mit der View Connection Server-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Desktops verwenden.

Wenn Sie Standardwerte für die Ablaufzeit von Kennwörtern und die Active Directory-Gruppenmitgliedschaft konfigurieren, werden diese Einstellungen von allen View Connection Server-Instanzen innerhalb einer Gruppe verwendet.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt View Manager ein Benutzerkonto für den Client in Active Directory. Wenn Sie einen Namen für einen Client angeben, muss dieser Name mit der Zeichenfolge „custom-“ oder einer der anderen Zeichenfolgen beginnen, die Sie in ADAM definieren können, außerdem darf diese Zeichenfolge nicht länger als 20 Zeichen lang sein. Verwenden Sie einen angegebenen Namen nicht mit mehreren Clientgeräten.

Unter `pae-ClientAuthPrefix`, einem Attribut mit mehreren Werten, können Sie alternative Präfixe angeben, und zwar unter `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM in einer View Connection Server-Instanz. Vermeiden Sie, diese Präfixe bei normalen Benutzerkonten zu verwenden.

Wenn Sie keinen Namen angeben, generiert View Manager einen Namen aus der für das Clientgerät angegebenen MAC-Adresse. Wenn die MAC-Adresse beispielsweise **[00:10:db:ee:76:80]** lautet, wird der Kontoname **[cm-00_10_db_ee_76_80]** generiert. Diese Konten können nur mit View Connection Server-Instanzen verwendet werden, die für die Authentifizierung von Clients aktiviert sind.

Einige Thin Clients lassen zur Verwendung mit dem Kiosk-Modus nur Kontennamen zu, die mit der Zeichenfolge „custom-“ oder „cm-“ beginnen.

Ein automatisch generiertes Kennwort umfasst 16 Zeichen, mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen sowie eine Zahl und kann sich wiederholende Zeichen enthalten. Wenn ein sichereres Kennwort erforderlich ist, muss das Kennwort über die Option `-password` angegeben werden.

Wenn Sie die Option `-group` zur Angabe einer Gruppe verwenden oder zuvor eine Standardgruppe festgelegt haben, fügt View Manager das Clientkonto zu dieser Gruppe hinzu. Durch Angabe der Option `-nogroup` können Sie verhindern, dass das Konto zu einer Gruppe hinzugefügt wird.

Wenn Sie eine View Connection Server-Instanz für die Authentifizierung von Clients im Kiosk-Modus aktivieren, können Sie optional festlegen, dass Clients ein Kennwort bereitstellen müssen. Bei Deaktivierung der Authentifizierung können Clients keine Verbindung zu ihren Desktops herstellen.

Wenngleich die Authentifizierung für eine einzelne View Connection Server-Instanz aktiviert oder deaktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle View Connection Server-Instanzen innerhalb einer Gruppe. Ein Client muss nur einmal hinzugefügt werden, damit alle View Connection Server-Instanzen in einer Gruppe Anforderungen von diesem Client akzeptieren.

Wenn Sie beim Aktivieren der Authentifizierung die Option `-requirepassword` angeben, kann die View Connection Server-Instanz keine Clients authentifizieren, die über automatisch generierte Kennwörter verfügen. Wenn Sie die Konfiguration einer View Connection Server-Instanz ändern und diese Option angeben, können diese Clients nicht authentifiziert werden und der Fehler `Unknown username or bad password (Unbekannter Benutzername oder falsches Kennwort)` wird ausgegeben.

Optionen

Tabelle 17-14 zeigt die verfügbaren Optionen für die Konfiguration von Clients im Kiosk-Modus.

Tabelle 17-14. Optionen für die Konfiguration von Clients im Kiosk-Modus

Option	Beschreibung
`–add`	Fügt ein Konto für einen Client im Kiosk-Modus hinzu.
`–clientauth`	Gibt einen Vorgang zur Konfiguration der Authentifizierung für einen Client im Kiosk-Modus an.
`–clientid` *Client-ID*	Gibt den Namen oder die MAC-Adresse des Clients an.
`–description` "*Beschreibungstext*"	Erstellt eine Beschreibung des Kontos für das Clientgerät in Active Directory.
`–disable`	Deaktiviert die Authentifizierung von Clients im Kiosk-Modus auf einer angegebenen View Connection Server-Instanz.
`–domain` *Domänenname*	Gibt die Domäne des Kontos für das Clientgerät an.
`–enable`	Aktiviert die Authentifizierung von Clients im Kiosk-Modus auf einer angegebenen View Connection Server-Instanz.
`–expirepassword`	Gibt an, dass die Ablaufzeit für Kennwörter der Clientkonten mit der Ablaufzeit für die View Connection Server-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, laufen Kennwörter nicht ab.
`–force`	Deaktiviert die Bestätigungsmeldung beim Entfernen eines Kontos für einen Client im Kiosk-Modus.
`–genpassword`	Generiert ein Kennwort für das Clientkonto. Dies ist das Standardverhalten, wenn weder `–password` noch `–genpassword` angegeben wird.
`–getdefaults`	Ruft die Standardwerte für das Hinzufügen von Clientkonten ab.
`–group` *Gruppenname*	Gibt den Namen der Standardgruppe an, zu der Clientkonten hinzugefügt werden. Der Name der Gruppe muss als der Prä-Windows 2000-Gruppenname aus Active Directory angegeben werden.
`–list`	Zeigt Informationen zu Clients im Kiosk-Modus sowie zu View Connection Server-Instanzen an, auf denen die Authentifizierung von Clients im Kiosk-Modus aktiviert ist.
`–noexpirepassword`	Gibt an, dass das Kennwort für ein Konto nicht abläuft.
`–nogroup`	Beim Hinzufügen eines Kontos für einen Client gibt diese Option an, dass das Clientkonto nicht zur Standardgruppe hinzugefügt wird. Beim Festlegen der Standardwerte für Clients löscht diese Option die Einstellung für die Standardgruppe.
`–ou` *DN*	Gibt den Distinguished Name der Organisationseinheit an, zu der Clientkonten hinzugefügt werden. Beispiel: OU=kiosk-ou,DC=myorg,DC=com **Hinweis** Die Konfiguration einer Organisationseinheit kann nicht über die Option `–setdefaults` geändert werden.
`–password` "*Kennwort*"	Gibt ein explizites Kennwort für das Clientkonto an.
`–remove`	Entfernt das Konto für einen Client im Kiosk-Modus.
`–removeall`	Entfernt die Konten aller Clients im Kiosk-Modus.
`–requirepassword`	Gibt an, dass Clients im Kiosk-Modus Kennwörter bereitstellen müssen. View Manager akzeptiert für neue Verbindungen keine generierten Kennwörter.
`–s` *Verbindungsserver*	Gibt den NetBIOS-Namen der View Connection Server-Instanz an, für welche die Authentifizierung von Clients im Kiosk-Modus aktiviert oder deaktiviert werden soll.

Tabelle 17-14. Optionen für die Konfiguration von Clients im Kiosk-Modus (Fortsetzung)

Option	Beschreibung
`–setdefaults`	Legt die Standardwerte für das Hinzufügen von Clientkonten fest.
`–update`	Aktualisiert ein Konto für einen Client im Kiosk-Modus.

Beispiele

Legen Sie die Standardwerte für die Organisationseinheit, den Ablauf von Kennwörtern sowie die Gruppenmitgliedschaft von Clients fest.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group
kc–grp
```

Rufen Sie die aktuellen Standardwerte für Clients im Textformat ab.

```
vdmadmin –Q –clientauth –getdefaults
```

Rufen Sie die aktuellen Standardwerte für Clients im XML-Format ab.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne **[MYORG]** hinzu und verwenden Sie die Standardeinstellungen für die Gruppe **[kc-grp]** .

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne **[MYORG]** hinzu und verwenden Sie ein automatisch generiertes Kennwort.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou "OU=kiosk–
ou,DC=myorg,DC=com" –group kc–grp
```

Fügen Sie ein Konto für einen benannten Client hinzu und geben Sie ein Kennwort zur Verwendung mit dem Client an.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Aktualisieren Sie ein Konto für einen Client und geben Sie ein neues Kennwort sowie eine Beschreibung an.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –
description "Foyer Entry Workstation"
```

Entfernen Sie das Konto für einen Kiosk-Client, der über seine MAC-Adresse angegeben wird, aus der Domäne **[MYORG]** .

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Entfernen Sie die Konten aller Clients, ohne eine Bestätigungsmeldung für den Entfernungsvorgang anzuzeigen.

```
vdmadmin –Q –clientauth –removeall –force
```

Aktivieren Sie die Authentifizierung von Clients für die View Connection Server-Instanz **[csvr-2]** . Clients mit automatisch generierten Kennwörtern können sich ohne Angabe eines Kennworts authentifizieren.

```
vdmadmin –Q –enable –s csvr–2
```

Aktivieren Sie die Authentifizierung von Clients für die View Connection Server-Instanz **[csvr-3]** und legen Sie fest, dass die Clients ihre Kennwörter für View Client bereitstellen müssen. Clients mit automatisch generierten Kennwörtern können sich nicht authentifizieren.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Deaktivieren Sie die Authentifizierung von Clients für die View Connection Server-Instanz **[csvr-1]** .

```
vdmadmin –Q –disable –s csvr–1
```

Zeigen Sie Informationen zu Clients im Textformat an. Der Client **[cm-00_0c_29_0d_a3_e6]** verfügt über ein automatisch generiertes Kennwort, sodass dieses Kennwort nicht durch den Endbenutzer oder über ein Anwendungsskript angegeben werden muss. Der Client **[cm-00_22_19_12_6d_cf]** verfügt über ein explizit angegebenes Kennwort, sodass der Endbenutzer dieses Kennwort angeben muss. Die View Connection Server-Instanz **[CONSVR2]** akzeptiert Authentifizierungsanforderungen von Clients mit automatisch generierten Kennwörtern. **[CONSVR1]** akzeptiert keine Authentifizierungsanforderungen von Clients im Kiosk-Modus.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Anzeigen des ersten Benutzers eines Desktops unter Verwendung der Option „-R“

Sie können den Befehl `vdmadmin` mit der Option `–R` verwenden, um die anfängliche Zuweisung eines verwalteten Desktops zu ermitteln. Bei Verlust von LDAP-Daten wird diese Information z.B. möglicherweise benötigt, um eine Neuzuweisung von Desktops zu Benutzern durchzuführen.

Syntax

```
vdmadmin –R –i Netzwerkadresse
```

Nutzungshinweise

Die Option `–b` kann nicht verwendet werden, um diesen Befehl als Benutzer mit Administratorrechten auszuführen. Sie müssen als Benutzer mit der Rolle **Administrator** angemeldet sein.

Options (Optionen)

Die Option `–i` gibt die IP-Adresse des Desktops an.

Beispiele

Zeigen Sie den ersten Benutzer an, der über die IP-Adresse **[10.20.34.120]** auf die Maschine zugegriffen hat.

```
vdmadmin –R –i 10.20.34.120
```

Entfernen des Eintrags für eine View Connection Server-Instanz unter Verwendung der Option „-S“

Sie können den Befehl `vdmadmin` mit der Option `–S` verwenden, um den Eintrag für eine View Connection Server-Instanz aus der View Manager-Konfiguration zu entfernen.

Syntax

```
vdmadmin –S [–b Authentifizierungsargumente] –r –s Server
```

Nutzungshinweise

Um Hochverfügbarkeit zu gewährleisten, ermöglicht View Manager die Konfiguration einer oder mehrerer View Connection Server-Replikatinstanzen in einer View Connection Server-Gruppe. Wenn Sie eine View Connection Server-Instanz in einer Gruppe deaktivieren, bleibt der Eintrag für den Server in der View Manager-Konfiguration erhalten.

Führen Sie die folgenden Schritte aus, um den Eintrag dauerhaft zu entfernen:

1. Deinstallieren Sie die View Connection Server-Instanz vom Windows Server-Computer, indem Sie das View Connection Server-Installationsprogramm ausführen.
2. Entfernen Sie die ADAM-Instanz VMwareVDMDS vom Windows Server-Computer, indem Sie das Dienstprogramm **[Add/Remove Programs (Software)]** ausführen.
3. Verwenden Sie den Befehl `vdmadmin` auf einer anderen View Connection Server-Instanz, um den Eintrag für die deinstallierte View Connection Server-Instanz aus der Konfiguration zu entfernen.

Wenn Sie VMware View auf den entfernten Systemen erneut installieren möchten, ohne die View-Konfiguration der ursprünglichen Gruppe zu replizieren, starten Sie vor der erneuten Installation alle View Connection Server-Hosts in der ursprünglichen Gruppe. Dadurch wird verhindert, dass die erneut installierten View Connection Server-Instanzen die Konfigurationsaktualisierungen ihrer ursprünglichen Gruppe erhalten.

Options (Optionen)

Die Option `–s` gibt den NetBIOS-Namen der View Connection Server-Instanz an, die entfernt werden soll.

Beispiele

Entfernen Sie den Eintrag für die View Connection Server-Instanz **[connsvr3]** .

```
vdmadmin –S –r –s connsvr3
```

Festlegen einer maximalen Größe für Paketdateien mithilfe der Option „-T“, um View Transfer Server-Pakete bei der Veröffentlichung zu unterteilen

Sie können über den Befehl `vdmadmin` mit der Option –T eine maximale Größe festlegen, ab der View Transfer Server-Pakete bei der Veröffentlichung unterteilt werden. Sie sollten einen Grenzwert festlegen, wenn Sie einen Proxy-Cache verwenden, für den eine maximale Objektgröße definiert ist.

Syntax

`vdmadmin –T [–packagelimit` *`Größe`*`]`

Nutzungshinweise

In einem Netzwerk mit Proxy-Cache können Sie die Leistung steigern, indem Sie die Größe der veröffentlichten View Transfer Server-Paketdateien so begrenzen, dass diese die maximale vom Cache vorgegebene Objektgröße nicht überschreiten. Wenn Sie einen maximale Größe festlegen, unterteilt View Transfer Server eine Paketdatei in kleinere Dateien, die diese maximale Größe nicht überschreiten.

Optionen

Die Option `–packagelimit` legt die maximale Größe in Byte fest, ab der die Dateien unterteilt werden. Wenn Sie diese Option nicht festlegen, gibt der Befehl den aktuellen Grenzwert zurück.

Beispiele

Legen Sie eine maximale Größe von 100MB fest, ab der die Dateien unterteilt werden.

```
vdmadmin –T –packagelimit 104857600
```

Zeigen Sie die aktuelle maximale Größe an, ab der die Dateien unterteilt werden.

```
vdmadmin –T
```

Anzeigen von Informationen zu Benutzern unter Verwendung der Option „-U“

Sie können den Befehl `vdmadmin` mit der Option `–U` verwenden, um detaillierte Informationen zu Benutzern anzuzeigen.

Syntax

`vdmadmin –U [–b` *`Authentifizierungsargumente`*`] –u` *`Domäne\Benutzer`* `[–w | –n] [–xml]`

Nutzungshinweise

Der Befehl zeigt Informationen zu einem Benutzer aus Active Directory und View Manager an.

- Active Directory-Informationen zum Konto des Benutzers.
- Mitgliedschaft in Active Directory-Gruppen.
- Desktop-Berechtigungen, einschließlich Desktop-ID, Anzeigename, Beschreibung, Ordner und Informationen dazu, ob ein Desktop deaktiviert wurde.
- ThinApp-Zuweisungen.

- Administratorrollen, u. a. die Administratorrechte eines Benutzers sowie die Ordner, für die diese Rechte gelten.

Options (Optionen)

Die Option `–u` gibt den Namen und die Domäne des Benutzers an.

Beispiele

Zeigen Sie Informationen zum Benutzer **[Jo]** in der Domäne **[CORP]** im XML-Format mit ASCII-Zeichen an.

```
vdmadmin –U –u CORP\Jo –n –xml
```

Entschlüsseln der virtuellen Maschine eines lokalen Desktops unter Verwendung der Option „-V“

VMware View schützt die virtuelle Maschine eines lokalen Desktops, indem das zugehörige Basis-Image verschlüsselt wird. Wenn es nicht möglich ist, den lokalen Desktop einzuschalten oder einzuchecken, können Sie den Befehl `vdmadmin` mit der Option `–V` dazu verwenden, die virtuelle Maschine zu entschlüsseln, um Daten aus dieser wiederherzustellen.

Syntax

```
vdmadmin –V –rescue [–b Authentifizierungsargumente] –d Desktop –u Domäne\Benutzer –infile
Pfad_zu_VM–Datei
```

Nutzungshinweise

Zum Entschlüsseln einer vollständigen virtuellen Maschine kopieren Sie alle Dateien der virtuellen Maschine vom Clientcomputer. Geben Sie den Namen der Konfigurationsdatei für die virtuelle VMware-Maschine (VMX-Datei) als Argument der Option `–infile` an.

Zum Entschlüsseln einer einzelnen Festplatte einer virtuellen Maschine kopieren Sie alle virtuellen VMware-Festplattendateien (VMDK-Dateien), die dieser Festplatte entsprechen. Wenn Sie den lokalen Desktop aus einem Linked-Clone-Desktop erstellt haben, müssen Sie auch den Unterordner kopieren, der die VMDK-Dateien für das Basis-Image enthält. Geben Sie den Namen der VMDK-für die Festplatte als Argument der Option `–infile` an. Geben Sie keine VMDK-Datei an, die einem Festplatten-Slice entspricht.

Der Befehl `vdmadmin` schreibt die entschlüsselten Dateien in einen Unterordner namens `rescued`.

Die Entschlüsselung schlägt fehl, wenn in der View LDAP-Konfiguration nicht der richtige Authentifizierungsschlüssel vorhanden ist oder wenn eine erforderliche Datei der virtuellen Maschine beschädigt ist oder fehlt.

Options (Optionen)

Tabelle 17-15 zeigt die Optionen, die Sie zum Entschlüsseln einer vollständigen virtuellen Maschine oder einer ihrer Festplatten angeben müssen.

Tabelle 17-15. Optionen zum Entschlüsseln der virtuellen Maschine eines lokalen Desktops

Option	Beschreibung
`–d` *Desktop*	Legt den Namen des Desktop-Pools fest.
`–infile` *Pfad_zu_VM-Datei*	Gibt den Pfad zur VMX- oder VMDK-Datei der virtuellen Maschine für den lokalen Desktop an.
`–u` *Domäne\Benutzer*	Gibt die Domäne und den Namen des Endbenutzers für den lokalen Desktop an.

Beispiele

Entschlüsseln Sie eine vollständige virtuelle Maschine durch Angeben der zugehörigen VMX-Datei.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile "J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Appli-
cations,DC=mycorp,DC=com.vmx"
```

Entschlüsseln Sie die aktuelle Version der Festplatte `scsi00` der virtuellen Maschine durch Angeben der zugehörigen VMDK-Datei.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile "J:\Temp\LMDT_Reco-
very\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk"
```

Entsperren oder Sperren von virtuellen Maschinen unter Verwendung der Option „-V“

Sie können den Befehl `vdmadmin` mit der Option `–V` verwenden, um virtuelle Maschinen im Rechenzentrum zu sperren oder zu entsperren.

Syntax

```
vdmadmin –V [–b Authentifizierungsargumente] –e –d Desktop –m Maschine [–m Maschine] ...
vdmadmin –V [–b Authentifizierungsargumente] –e –vcdn vCenter-DN –vmpath Pfad_Bestandsliste
vdmadmin –V [–b Authentifizierungsargumente] –p –d Desktop –m Maschine [–m Maschine] ...
vdmadmin –V [–b Authentifizierungsargumente] –p –vcdn vCenter-DN –vmpath Pfad_Bestandsliste
```

Nutzungshinweise

Sie sollten ausschließlich den Befehl `vdmadmin` zum Entsperren oder Sperren einer virtuellen Maschine verwenden, wenn ein Problem dazu geführt hat, dass sich ein View-Desktop in einem fehlerhaften Zustand befindet. Verwenden Sie den Befehl nicht zur Verwaltung von Desktops, die ordnungsgemäß funktionieren. Verwenden Sie `vdmadmin` beispielsweise nicht, um einen ausgecheckten Remote-Desktop zu entsperren, wenn Sie mit View Administrator ein Rollback der lokalen Sitzung durchführen können.

Wenn ein Desktop gesperrt ist, für diesen kein Rollback durchgeführt werden kann und in ADAM der Eintrag für die zugehörige virtuelle Maschine vorhanden ist, können Sie über die Optionen `–d` und `–m` den Desktop-Pool und die virtuelle Maschine für den Remote-Desktop angeben, den Sie entsperren möchten. Über den Befehl `vdmadmin –M` können Sie den Namen der virtuellen Maschine ermitteln, die einem Benutzer zugewiesen ist.

Wenn ein Desktop gesperrt ist und der Eintrag für die zugehörige virtuelle Maschine nicht mehr in ADAM vorhanden ist, können Sie den Bestandslistenpfad der virtuellen Maschine und den vCenter Server über die Optionen `–vmpath` und `–vcdn` angeben. Mithilfe von vCenter Client können Sie den Bestandslistenpfad der virtuellen Maschine für einen Desktop oder eine View Transfer Server-Instanz unter `Home/Bestandsliste/VMs und Vorlagen` ermitteln. Sie können in ADAM das Dienstprogramm ADSI-Editor verwenden, um den Distinguished Name der vCenter Server-Instanz unter der Überschrift `OU=Properties` zu suchen.

Options (Optionen)

Tabelle 17-16 zeigt die Optionen, die Sie zum Entsperren oder Sperren von virtuellen Maschinen angeben können.

Tabelle 17-16. Optionen für das Entsperren oder Sperren von virtuellen Maschinen

Option	Beschreibung
`–d` *Desktop*	Gibt den Desktop-Pool an.
`–e`	Entsperrt eine virtuelle Maschine.
`–m` *Maschine*	Legt den Namen der virtuellen Maschine fest.
`–p`	Sperrt eine virtuelle Maschine.
`–vcdn` *vCenter-DN*	Gibt den Distinguished Name der vCenter Server-Instanz an.
`–vmpath` *Pfad_Bestandsliste*	Legt den Bestandslistenpfad der virtuellen Maschine fest.

Beispiele

Entsperren Sie die virtuellen Maschinen **[machine1]** und **[machine2]** im Desktop-Pool **[dtpool3]** .

```
vdmadmin –V –e –d dtpool3 –m machine1 –m machine2
```

Entsperren Sie die virtuelle Maschine für eine View Transfer Server-Instanz auf einer vCenter Server-Instanz.

```
vdmadmin –V –e –vcdn  "CN=f1060058–dde2–4940–947b–5d83757b1787,OU=VirtualCenter,OU=Proper–
ties,DC=myorg,DC=com" –vmpath "/DataCenter1/vm/Desktops/LocalMode/LDwin7"
```

Sperren Sie die virtuelle Maschine **[machine3]** im Desktop-Pool **[dtpool3]** .

```
vdmadmin –V –p –d dtpool3 –m machine3
```

Ermitteln und Lösen von Konflikten bei LDAP-Einträgen mit der Option „-X“

Sie können den Befehl `vdmadmin` mit der Option –X verwenden, um Konflikte bei LDAP-Einträgen auf replizierten View Connection Server-Instanzen in einer Gruppe zu ermitteln und zu lösen.

Syntax

```
vdmadmin –X [–b Authentifizierungsargumente] –collisions [–resolve]
```

Nutzungshinweise

Wenn auf mindestens zwei View Connection Server-Instanzen dieselben LDAP-Einträge erstellt wurden, kann dies zu Integritätsproblemen von LDAP in View führen. Dies kann passieren, wenn ein Upgrade durchgeführt wird, während die LDAP-Replikation nicht verwendet wird. Auch wenn View Manager in regelmäßigen Abständen nach dieser Fehlerbedingung sucht, können Sie den Befehl `vdmadmin` auf den View Connection Server-Instanzen in der Gruppe ausführen, um Konflikte bei LDAP-Einträgen manuell zu ermitteln und diese zu lösen.

Options (Optionen)

Tabelle 17-17 zeigt die Optionen, die Sie angeben können, um Konflikte bei LDAP-Einträgen zu ermitteln und zu lösen.

Tabelle 17-17. Optionen zum Ermitteln und Lösen von Konflikten bei LDAP-Einträgen

Option	Beschreibung
`–collisions`	Legt einen Vorgang zum Ermitteln von LDAP-Konflikten in einer View Connection Server-Gruppe fest.
`–resolve`	Löst alle ermittelten LDAP-Konflikte.

Beispiele

Ermitteln Sie Konflikte bei LDAP-Einträgen in einer View Connection Server-Gruppe.

```
vdmadmin –X –collisions
```

Ermitteln und lösen Sie Konflikte bei LDAP-Einträgen.

```
vdmadmin –X –collisions –resolve
```

Einrichten von Clients im Kiosk-Modus

18

Sie können unbeaufsichtigte Clients einrichten, die über VMware View auf ihre Desktops zugreifen können.

Ein Client im Kiosk-Modus ist ein Thin Client oder ein PC mit eingeschränkten Funktionen, auf dem View Client ausgeführt wird, um die Verbindung mit einer View Connection Server-Instanz herzustellen und eine Remote-Sitzung zu starten. Endbenutzer müssen sich typischerweise nicht für den Zugriff auf das Clientgerät anmelden. Der Desktop fordert für einige Anwendungen jedoch möglicherweise Authentifizierungsinformationen an. Beispiele sind Arbeitsstationen zur Eingabe medizinischer Daten, Check-in-Schalter, Selbstbedienungsstationen und Informationsterminals mit öffentlichem Zugriff.

Sie sollten sicherstellen, dass die Desktop-Anwendung Authentifizierungsmechanismen für sichere Transaktionen implementiert, das physische Netzwerk gegen das Manipulieren und Ausspähen von Daten geschützt ist und alle mit dem Netzwerk verbundenen Geräte als vertrauenswürdig eingestuft werden.

Clients im Kiosk-Modus unterstützen die eigenständigen Funktionen für den Remote-Zugriff, z.B. die Umleitung von USB-Geräten an die Remote-Sitzung und die standortbasierte Druckfunktion.

View Manager verwendet die Funktion zur flexiblen Authentifizierung in VMware View 4.5 und höher, um anstelle des Endbenutzers ein Clientgerät im Kiosk-Modus zu authentifizieren. Eine View Connection Server-Instanz kann für die Authentifizierung von Clients konfiguriert werden, die über ihre MAC-Adresse oder einen Benutzernamen identifiziert werden, der mit der Zeichenfolge „custom-“ oder einer anderen Präfixzeichenfolge beginnt, die Sie in ADAM definiert haben. Wenn für einen Client das automatische Generieren eines Kennworts konfiguriert ist, kann View Client auf dem Gerät ohne Angabe eines Kennworts ausgeführt werden. Bei Konfiguration eines expliziten Kennworts muss dieses Kennwort für View Client angegeben werden. Da View Client normalerweise über ein Skript ausgeführt und das Kennwort als Klartext angezeigt würde, sollten Sie sicherstellen, dass das Skript nicht von Benutzern ohne entsprechende Berechtigung gelesen werden kann.

Nur View Connection Server-Instanzen, die für die Authentifizierung von Clients im Kiosk-Modus aktiviert wurden, können Verbindungen von Konten akzeptieren, deren Namen mit den Zeichen „cm-“ (gefolgt von einer MAC-Adresse) oder mit den Zeichen „Custom-“ oder einer alternativen Zeichenfolge beginnen, die Sie definiert haben. Die manuelle Eingabe von Benutzernamen mit diesen Formaten ist bei View Client in VMware View 4.5 und höher nicht zulässig.

Die empfohlene Vorgehensweise ist das Verwenden dedizierter View Connection Server-Instanzen zur Verarbeitung von Clients im Kiosk-Modus und das Erstellen dedizierter Organisationseinheiten und Gruppen in Active Directory für die Konten dieser Clients. Bei dieser Vorgehensweise werden die Systeme nicht nur partitioniert und gegen unberechtigten Zugriff geschützt, sondern gleichzeitig wird die Konfiguration und Verwaltung der Clients vereinfacht.

Konfigurieren von Clients im Kiosk-Modus

Zur Konfiguration von Active Directory und View Manager für die Unterstützung von Clients im Kiosk-Modus müssen mehrere Aufgaben mit einer bestimmten Reihenfolge ausgeführt werden.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Ausführen der Konfigurationsaufgaben verfügen.

- **Domain Admins (Domänen-Admins)** oder **Account Operators (Konten-Operatoren)** – die Anmeldeinformationen dieser Gruppen sind erforderlich, um in Active Directory Änderungen an Konten von Benutzern und Gruppen in einer Domäne vorzunehmen.
- **Administrators (Administratoren)**, **Inventory Administrators (Bestandslistenadministratoren)**oder eine äquivalente Rolle – diese Rollen sind erforderlich, um View Administrator zum Berechtigen von Benutzern oder Gruppen für Desktops zu verwenden.
- **Administrators (Administratoren)** oder eine äquivalente Rolle – diese Rollen sind erforderlich, um den Befehl `vdmadmin` ausführen zu können.

Vorgehensweise

1 Vorbereiten von Active Directory und View Manager für Clients im Kiosk-Modus auf Seite 415

Active Directory muss für das Akzeptieren der Konten konfiguriert werden, die zur Authentifizierung von Clientgeräten erstellt werden. Beim Erstellen einer Gruppe muss die Gruppe zudem für den Desktop-Pool berechtigt werden, auf den ein Client zugreift. Der von den Clients verwendete Desktop-Pool kann ebenfalls vorbereitet werden.

2 Festlegen von Standardwerten für Clients im Kiosk-Modus auf Seite 416

Mithilfe des Befehls `vdmadmin` können Sie die Standardwerte für eine Organisationseinheit, die Ablaufzeit von Kennwörtern sowie Gruppenmitgliedschaften in Active Directory für Clients im Kiosk-Modus festlegen.

3 Anzeigen der MAC-Adressen von Clientgeräten auf Seite 417

Wenn Sie basierend auf der MAC-Adresse ein Konto für einen Client erstellen möchten, können Sie die MAC-Adresse des Clientgeräts mit View Client ermitteln.

4 Hinzufügen von Konten für Clients im Kiosk-Modus auf Seite 417

Mithilfe des Befehls `vdmadmin` können Clientkonten zur Konfiguration einer View Connection Server-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer View Connection Server-Instanz verwendet werden, auf der die Authentifizierung von Clients aktiviert ist. Zudem können Sie die Konfiguration von Clients aktualisieren oder die Clientkonten aus dem System entfernen.

5 Aktivieren der Authentifizierung von Clients im Kiosk-Modus auf Seite 419

Mithilfe des Befehls `vdmadmin` kann die Authentifizierung von Clients aktiviert werden, die versuchen, über eine View Connection Server-Instanz eine Verbindung mit ihren Desktops herzustellen.

6 Überprüfen der Konfiguration von Clients im Kiosk-Modus auf Seite 420

Mithilfe des Befehls `vdmadmin` können Informationen zu Clients im Kiosk-Modus und zu View Connection Server-Instanzen angezeigt werden, die zur Authentifizierung dieser Clients konfiguriert sind.

7 Verbinden mit Desktops über Clients im Kiosk-Modus auf Seite 421

Sie können View Client über die Befehlszeile ausführen oder ein Skript verwenden, um einen Client mit einer Remote-Sitzung zu verbinden.

Vorbereiten von Active Directory und View Manager für Clients im Kiosk-Modus

Active Directory muss für das Akzeptieren der Konten konfiguriert werden, die zur Authentifizierung von Clientgeräten erstellt werden. Beim Erstellen einer Gruppe muss die Gruppe zudem für den Desktop-Pool berechtigt werden, auf den ein Client zugreift. Der von den Clients verwendete Desktop-Pool kann ebenfalls vorbereitet werden.

Die empfohlene Vorgehensweise sieht das Erstellen einer separaten Organisationseinheit und Gruppe vor, um den Verwaltungsaufwand für Clients im Kiosk-Modus zu minimieren. Sie können einzelne Konten für Clients hinzufügen, die keiner Gruppe angehören, bei Konfiguration einer größeren Anzahl an Clients führt dies jedoch zu einem erheblichen Verwaltungsaufwand.

Vorgehensweise

1 Erstellen Sie in Active Directory eine separate Organisationseinheit und Gruppe für Clients im Kiosk-Modus.

   Für die Gruppe muss ein Prä-Windows 2000-Name angegeben werden. Dieser Name wird zur Identifizierung der Gruppe gegenüber dem Befehl `vdmadmin` verwendet.

2 Erstellen Sie das Image oder die Vorlage für die virtuelle Gastmaschine.

   Sie können eine virtuelle Maschine, die von vCenter Server verwaltet wird, als Vorlage für einen automatisierten Pool, als übergeordnetes Element für einen Linked-Clone-Pool oder als Desktop-Quelle für einen manuellen Pool verwenden. Zudem können Sie Anwendungen in der virtuellen Gastmaschine installieren und konfigurieren.

3 Konfigurieren Sie die virtuelle Gastmaschine so, dass die Clients bei unbeaufsichtigtem Betrieb nicht gesperrt werden.

   View unterdrückt die Prä-Anmeldenachricht für Clients, die eine Verbindung im Kiosk-Modus herstellen. Wenn es erforderlich ist, dass ein Ereignis den Bildschirm entsperrt und eine Meldung anzeigt, können Sie eine geeignete Anwendung auf der virtuellen Maschine des Gasts konfigurieren.

4 Erstellen Sie in View Administrator den von den Clients verwendeten Desktop-Pool und berechtigen Sie die Gruppe für diesen Pool.

   Möglicherweise entscheiden Sie sich zur Erstellung eines Linked-Clone-Desktop-Pools mit dynamischer Zuweisung, da diese Art von Pool sich am besten für die Anforderungen Ihrer Clientanwendung eignet. Sie können zudem eine oder mehrere ThinApp-Anwendungen mit dem Desktop-Pool verknüpfen.

   Wichtig Berechtigen Sie einen Client oder eine Gruppe nicht für mehrere Desktop-Pools. Anderenfalls weist View Manager nach dem Zufallsprinzip einen Desktop aus den Pools zu, für die ein Client berechtigt ist, und es wird eine Warnung generiert.

5 Wenn für die Clients der standortbasierte Druck eingerichtet werden soll, konfigurieren Sie die Active Directory-Gruppenrichtlinieneinstellung `AutoConnect Location-based Printing for VMware View (Automatische standortbasierte Druckfunktion für VMware View)`, die sich im Gruppenrichtlinienobjekt-Editor von Microsoft im Ordner `Software Settings (Softwareeinstellungen)` unterhalb von `Computer Configuration (Computerkonfiguration)` befindet.

6 Konfigurieren Sie andere erforderliche Richtlinien, um die View-Desktops der Clients zu optimieren und zu schützen.

   Beispielsweise kann es sinnvoll sein, die Richtlinien zum Verbinden lokaler USB-Geräte mit dem Desktop außer Kraft zu setzen, wenn der Desktop gestartet oder die Geräte verbunden werden. View Client für Windows aktiviert diese Richtlinien standardmäßig für Clients im Kiosk-Modus.

Beispiel: Vorbereiten von Active Directory für Clients im Kiosk-Modus

Ein Unternehmensintranet verfügt über eine Domäne **[MYORG]** und eine Organisationseinheit mit dem Distinguished Name **[OU=myorg-ou,DC=myorg,DC=com]** . Erstellen Sie in Active Directory die Organisationseinheit **[kiosk-ou]** mit dem Distinguished Name **[OU=kiosk-ou,DC=myorg,DC=com]** und die Gruppe **[kc-grp]** zur Verwendung mit Clients im Kiosk-Modus.

Weiter

Legen Sie Standardwerte für die Clients fest.

Festlegen von Standardwerten für Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` können Sie die Standardwerte für eine Organisationseinheit, die Ablaufzeit von Kennwörtern sowie Gruppenmitgliedschaften in Active Directory für Clients im Kiosk-Modus festlegen.

Der Befehl `vdmadmin` muss für eine der View Connection Server-Instanzen in der Gruppe mit der View Connection Server-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Desktops verwenden.

Wenn Sie Standardwerte für die Ablaufzeit von Kennwörtern und die Active Directory-Gruppenmitgliedschaft konfigurieren, werden diese Einstellungen von allen View Connection Server-Instanzen innerhalb einer Gruppe verwendet.

Vorgehensweise

- Legen Sie die Standardwerte für Clients fest.

  ```
  vdmadmin –Q –clientauth –setdefaults [–b Authentifizierungsargumente] [–ou DN]
  [ –expirepassword | –noexpirepassword ] [–group Gruppenname | –nogroup]
  ```

Option	Beschreibung
–expirepassword	Gibt an, dass die Ablaufzeit für Kennwörter der Clientkonten mit der Ablaufzeit für die View Connection Server-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, laufen Kennwörter nicht ab.
–group *Gruppenname*	Gibt den Namen der Standardgruppe an, zu der Clientkonten hinzugefügt werden. Der Name der Gruppe muss als der Prä-Windows 2000-Gruppenname aus Active Directory angegeben werden.
–noexpirepassword	Gibt an, dass Kennwörter für Clientkonten nicht ablaufen.
–nogroup	Löscht die Einstellung für die Standardgruppe.
–ou *DN*	Gibt den Distinguished Name der standardmäßigen Organisationseinheit an, zu der Clientkonten hinzugefügt werden. Beispiel: OU=kiosk-ou,DC=myorg,DC=com **Hinweis** Die Konfiguration einer Organisationseinheit kann nicht über diesen Befehl geändert werden.

Der Befehl aktualisiert die Standardwerte für Clients in der View Connection Server-Gruppe.

Beispiel: Festlegen von Standardwerten für Clients im Kiosk-Modus

Legen Sie die Standardwerte für die Organisationseinheit, den Ablauf von Kennwörtern sowie die Gruppenmitgliedschaft von Clients fest.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group
kc–grp
```

Weiter

Ermitteln Sie die MAC-Adressen von Clientgeräten, die sich über ihre MAC-Adresse authentifizieren.

Anzeigen der MAC-Adressen von Clientgeräten

Wenn Sie basierend auf der MAC-Adresse ein Konto für einen Client erstellen möchten, können Sie die MAC-Adresse des Clientgeräts mit View Client ermitteln.

Voraussetzungen

Melden Sie sich an der Clientkonsole an.

Vorgehensweise

- Zum Anzeigen der MAC-Adresse geben Sie den geeigneten Befehl für Ihre Plattform ein.

Option	Aktion
Windows	Geben Sie **`C:\Programme\VMware\VMware View\Client\bin\wswc -printEnvironmentInfo`** ein. View Client verwendet die konfigurierte standardmäßige View Connection Server-Instanz. Wenn Sie keinen Standardwert konfiguriert haben, werden Sie von View Client zur Angabe des Werts aufgefordert. Der Befehl zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
Linux	Geben Sie **`vmware-view --printEnvironmentInfo -s`** ***`Verbindungsserver`*** ein. Sie müssen die IP-Adresse oder den FQDN der View Connection Server-Instanz angeben, die View Client zur Herstellung einer Verbindung mit dem Desktop verwendet. Der Befehl zeigt die IP-Adresse, die MAC-Adresse, den Maschinennamen, die Domäne, den Namen und die Domäne angemeldeter Benutzer sowie die Zeitzone des Clientgeräts an.

Weiter

Fügen Sie Konten für die Clients hinzu.

Hinzufügen von Konten für Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` können Clientkonten zur Konfiguration einer View Connection Server-Gruppe hinzugefügt werden. Nach dem Hinzufügen eines Clients kann dieser mit einer View Connection Server-Instanz verwendet werden, auf der die Authentifizierung von Clients aktiviert ist. Zudem können Sie die Konfiguration von Clients aktualisieren oder die Clientkonten aus dem System entfernen.

Der Befehl `vdmadmin` muss für eine der View Connection Server-Instanzen in der Gruppe mit der View Connection Server-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Desktops verwenden.

Beim Hinzufügen von Clients im Kiosk-Modus erstellt View Manager ein Benutzerkonto für den Client in Active Directory. Wenn Sie für einen Client einen Namen angeben, muss dieser Name mit einer erkannten Präfixzeichenfolge, z.B. „custom-“, oder einer alternativen, von Ihnen in ADAM definierten Präfixzeichenfolge beginnen und darf maximal 20 Zeichen umfassen. Wenn Sie keinen Namen angeben, generiert View Manager einen Namen aus der für das Clientgerät angegebenen MAC-Adresse. Wenn die MAC-Adresse beispielsweise **[00:10:db:ee:76:80]** lautet, wird der Kontoname **[cm-00_10_db_ee_76_80]** generiert. Diese Konten können nur mit View Connection Server-Instanzen verwendet werden, die für die Authentifizierung von Clients aktiviert sind.

Wichtig Verwenden Sie einen angegebenen Namen nicht für mehrere Clientgeräte. Diese Konfiguration wird in zukünftigen Releases möglicherweise nicht unterstützt.

Vorgehensweise

- Führen Sie den Befehl `vdmadmin` mit den Optionen `–domain` und `–clientid` aus, um die Domäne und den Namen oder die MAC-Adresse des Clients anzugeben.

  `vdmadmin –Q –clientauth –add [–b Authentifizierungsargumente] –domain Domänenname –clientid Client–ID [–password "Kennwort" | –genpassword] [–ou DN] [–expirepassword | –noexpirepassword] [–group Gruppenname | –nogroup] [–description "Beschreibungstext"]`

Option	Beschreibung
`–clientid` *Client-ID*	Gibt den Namen oder die MAC-Adresse des Clients an.
`–description` "*Beschreibungstext*"	Erstellt eine Beschreibung des Kontos für das Clientgerät in Active Directory.
`–domain` *Domänenname*	Gibt die Domäne für den Client an.
`–expirepassword`	Gibt an, dass die Ablaufzeit für das Kennwort des Clientkontos mit der Ablaufzeit für die View Connection Server-Gruppe übereinstimmt. Wenn für die Gruppe keine Ablaufzeit definiert ist, läuft das Kennwort nicht ab.
`–genpassword`	Generiert ein Kennwort für das Clientkonto. Dies ist das Standardverhalten, wenn weder `–password` noch `–genpassword` angegeben wird. Ein generiertes Kennwort umfasst 16 Zeichen, mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen sowie eine Zahl und kann sich wiederholende Zeichen enthalten. Wenn ein sichereres Kennwort erforderlich ist, geben Sie das Kennwort über die Option `–password` an.
`–group` *Gruppenname*	Gibt den Namen der Gruppe an, zu der das Clientkonto hinzugefügt wird. Der Name der Gruppe muss als der Prä-Windows 2000-Gruppenname aus Active Directory angegeben werden. Wenn zuvor eine Standardgruppe festgelegt wurde, wird das Clientkonto zu dieser Gruppe hinzugefügt.
`–noexpirepassword`	Gibt an, dass das Kennwort für das Clientkonto nicht abläuft.
`–nogroup`	Gibt an, dass das Clientkonto nicht zur Standardgruppe hinzugefügt wird.
`–ou` *DN*	Gibt den Distinguished Name der Organisationseinheit an, zu der das Clientkonto hinzugefügt wird. Beispiel: OU=kiosk-ou,DC=myorg,DC=com
`–password` "*Kennwort*"	Gibt ein explizites Kennwort für das Clientkonto an.

Der Befehl erstellt in Active Directory ein Benutzerkonto für den Client in der angegebenen Domäne und Gruppe (sofern vorhanden).

Beispiel: Hinzufügen von Konten für Clients

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne **[MYORG]** hinzu und verwenden Sie die Standardeinstellungen für die Gruppe **[kc-grp]** .

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Fügen Sie ein Konto für einen Client, der über die MAC-Adresse angegeben wird, zur Domäne **[MYORG]** hinzu und verwenden Sie ein automatisch generiertes Kennwort.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Fügen Sie ein Konto für einen benannten Client hinzu und geben Sie ein Kennwort zur Verwendung mit dem Client an.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Fügen Sie ein Konto für einen benannten Client hinzu, der ein automatisch generiertes Kennwort verwendet.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –ou "OU=kiosk–ou,DC=my–
org,DC=com" –description "Kiosk 11"
```

Weiter

Aktivieren Sie die Authentifizierung der Clients.

Aktivieren der Authentifizierung von Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` kann die Authentifizierung von Clients aktiviert werden, die versuchen, über eine View Connection Server-Instanz eine Verbindung mit ihren Desktops herzustellen.

Der Befehl `vdmadmin` muss für eine der View Connection Server-Instanzen in der Gruppe mit der View Connection Server-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Desktops verwenden.

Wenngleich die Authentifizierung für eine einzelne View Connection Server-Instanz aktiviert wird, gelten die anderen Einstellungen für die Clientauthentifizierung für alle View Connection Server-Instanzen innerhalb einer Gruppe. Das Konto für einen Client muss nur einmal hinzugefügt werden. Alle aktivierten View Connection Server-Instanzen innerhalb einer View Connection Server-Gruppe können den Client authentifizieren.

Vorgehensweise

- Aktivieren Sie die Authentifizierung von Clients für eine View Connection Server-Instanz.

  ```
  vdmadmin –Q –enable [–b Authentifizierungsargumente] –s Verbindungsserver [–requirepassword]
  ```

Option	Beschreibung
–requirepassword	Gibt an, dass Clients Kennwörter angeben müssen. **Wichtig** Bei Angabe dieser Option kann die View Connection Server-Instanz keine Clients authentifizieren, die über automatisch generierte Kennwörter verfügen. Wenn Sie die Konfiguration einer View Connection Server-Instanz ändern und diese Option angeben, können diese Clients nicht authentifiziert werden und der Fehler `Unknown username or bad password (Unbekannter Benutzername oder falsches Kennwort)` wird ausgegeben.
–s *Verbindungsserver*	Gibt den NetBIOS-Namen der View Connection Server-Instanz an, für welche die Authentifizierung von Clients aktiviert werden soll.

  Der Befehl aktiviert die angegebene View Connection Server-Instanz für die Authentifizierung von Clients.

Beispiel: Aktivieren der Authentifizierung von Clients im Kiosk-Modus

Aktivieren Sie die Authentifizierung von Clients für die View Connection Server-Instanz **[csvr-2]** . Clients mit automatisch generierten Kennwörtern können sich ohne Angabe eines Kennworts authentifizieren.

```
vdmadmin –Q –enable –s csvr–2
```

Aktivieren Sie die Authentifizierung von Clients für die View Connection Server-Instanz **[csvr-3]** und legen Sie fest, dass die Clients ihre Kennwörter für View Client bereitstellen müssen. Clients mit automatisch generierten Kennwörtern können sich nicht authentifizieren.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Weiter

Überprüfen Sie die Konfiguration der View Connection Server-Instanzen und Clients.

Überprüfen der Konfiguration von Clients im Kiosk-Modus

Mithilfe des Befehls `vdmadmin` können Informationen zu Clients im Kiosk-Modus und zu View Connection Server-Instanzen angezeigt werden, die zur Authentifizierung dieser Clients konfiguriert sind.

Der Befehl `vdmadmin` muss für eine der View Connection Server-Instanzen in der Gruppe mit der View Connection Server-Instanz ausgeführt werden, welche die Clients zum Herstellen einer Verbindung mit ihren Desktops verwenden.

Vorgehensweise

- Zeigen Sie Informationen zu Clients im Kiosk-Modus und zur Clientauthentifizierung an.

  `vdmadmin –Q –clientauth –list [–b` *`Authentifizierungsargumente`*`] [–xml]`

  Der Befehl zeigt Informationen zu Clients im Kiosk-Modus und zu den View Connection Server-Instanzen an, auf denen die Clientauthentifizierung aktiviert ist.

Beispiel: Anzeigen von Informationen für Clients im Kiosk-Modus

Zeigen Sie Informationen zu Clients im Textformat an. Der Client **[cm-00_0c_29_0d_a3_e6]** verfügt über ein automatisch generiertes Kennwort, sodass dieses Kennwort nicht durch den Endbenutzer oder über ein Anwendungsskript angegeben werden muss. Der Client **[cm-00_22_19_12_6d_cf]** verfügt über ein explizit angegebenes Kennwort, sodass der Endbenutzer dieses Kennwort angeben muss. Die View Connection Server-Instanz **[CONSVR2]** akzeptiert Authentifizierungsanforderungen von Clients mit automatisch generierten Kennwörtern. **[CONSVR1]** akzeptiert keine Authentifizierungsanforderungen von Clients im Kiosk-Modus.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Weiter

Stellen Sie sicher, dass sich die Clients mit ihren Desktops verbinden können.

Verbinden mit Desktops über Clients im Kiosk-Modus

Sie können View Client über die Befehlszeile ausführen oder ein Skript verwenden, um einen Client mit einer Remote-Sitzung zu verbinden.

Normalerweise würden Sie View Client unter Verwendung eines Befehlsskripts auf einem bereitgestellten Clientgerät ausführen.

Ein Beispielskript für die Ausführung von View Client auf einem Windows-System finden Sie unter `C:\Programme\VMware\VMware View\Client\bin\kiosk_mode.cmd`.

HINWEIS Auf einem Windows-Client werden USB-Geräte auf dem Client nicht automatisch weitergeleitet, wenn sie beim Start der Desktop-Sitzung von einer anderen Anwendung oder einem anderen Dienst verwendet werden. Stellen Sie sicher, dass die Treiber für alle Geräte, die weitergeleitet werden sollen, auf dem Client installiert sind. Sowohl auf Windows- als auch auf Linux-Clients werden Eingabegeräte (Human Interface Devices, HIDs) und Smartcard-Leser standardmäßig nicht weitergeleitet.

Vorgehensweise

- Zum Herstellen einer Verbindung mit einer Remote-Sitzung geben Sie den geeigneten Befehl für Ihre Plattform ein.

Option	Beschreibung
Windows	Geben Sie **`C:\Programmes\VMware\VMware View\Client\bin\wswc –unattended [–serverURL Verbindungsserver] [–userName Benutzername] [–password Kennwort] ein.`**
	`–password Kennwort` — Gibt das Kennwort für das Clientkonto an. Wenn ein Kennwort für das Konto definiert wurde, muss dieses Kennwort angegeben werden.
	`–serverURL Verbindungsserver` — Gibt die IP-Adresse oder den FQDN der View Connection Server-Instanz an, die View Client zur Herstellung einer Verbindung mit einem Desktop verwendet. Wenn Sie die IP-Adresse oder den FQDN der View Connection Server-Instanz, die View Client zum Herstellen einer Verbindung mit einem Desktop verwendet, nicht angeben, verwendet View Client die konfigurierte standardmäßige View Connection Server-Instanz.
	`–userName Benutzername` — Gibt den Namen des Clientkontos an. Wenn sich ein Client nicht über die MAC-Adresse, sondern unter Verwendung eines Kontonamens authentifizieren soll, der mit der erkannten Präfixzeichenfolge, z. B. „custom-“ beginnt, muss dieser Name angegeben werden.
Linux	Geben Sie **`vmware-view --unattended -s Verbindungsserver [--once] [-u Benutzername] [-p Kennwort] ein.`**
	`--once` — Gibt an, dass View Client bei einem Fehler nicht erneut versuchen soll, eine Verbindung herzustellen. **WICHTIG** Sie sollten diese Option normalerweise angeben und den Fehler anhand des Exitcodes behandeln. Anderenfalls kann es schwierig sein, den `vmware-view`-Prozess remote zu beenden.
	`-p Kennwort` — Gibt das Kennwort für das Clientkonto an. Wenn ein Kennwort für das Konto definiert wurde, muss dieses Kennwort angegeben werden.
	`-s Verbindungsserver` — Gibt die IP-Adresse oder den FQDN der View Connection Server-Instanz an, die View Client zur Herstellung einer Verbindung mit einem Desktop verwendet.
	`-u Benutzername` — Gibt den Namen des Clientkontos an. Wenn sich ein Client nicht über die MAC-Adresse, sondern unter Verwendung eines Kontonamens authentifizieren soll, der mit der erkannten Präfixzeichenfolge, z. B. „custom-“ beginnt, muss dieser Name angegeben werden.

Wenn View Manager den Kiosk-Client authentifiziert und ein View-Desktop verfügbar ist, startet der Befehl die Remote-Sitzung.

Beispiel: Ausführen von View Client auf Clients im Kiosk-Modus

Führen Sie View Client auf einem Windows-Client aus, dessen Kontoname auf der MAC-Adresse basiert und der über ein automatisch generiertes Kennwort verfügt.

```
C:\Programme\VMware\VMware View\Client\bin\wswc –unattended –serverURL consvr2.myorg.com
```

Führen Sie View Client auf einem Linux-Client aus, der einen zugewiesenen Namen und ein zugewiesenes Kennwort verwendet.

```
vmware–view –unattended –s 145.124.24.100 ––once –u custom–Terminal21 –p "Secret1!"
```

Ausführen von View Client über die Befehlszeile

19

View Client für Windows kann über die Befehlszeile oder über Skripts ausgeführt werden. Dies kann bei Implementierung einer Kiosk-basierten Anwendung sinnvoll sein, über die Endbenutzer auf Desktop-Anwendungen zugreifen können.

Verwenden Sie den Befehl `wswc`, um View Client für Windows über die Befehlszeile auszuführen. Der Befehl umfasst Optionen, mit denen sich das Verhalten von View Client ändern lässt.

Dieses Kapitel behandelt die folgenden Themen:

- „Verwenden von View Client-Befehlen“, auf Seite 425
- „View Client-Konfigurationsdatei“, auf Seite 427
- „View Client-Registrierungseinstellungen“, auf Seite 428
- „View Client-Exitcodes“, auf Seite 428

Verwenden von View Client-Befehlen

Die Syntax des Befehls `wswc` bestimmt, wie View Client ausgeführt wird.

Verwenden Sie den Befehl `wswc` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

`wswc [`*`Befehlszeilenoption`* `[`*`Argument`*`]] ...`

Über die angegebenen Befehlszeilenoptionen wird das Verhalten von View Client geändert.

Der Pfad zur ausführbaren Datei des Befehls `wswc` lautet standardmäßig `C:\Programme\VMware\VMware View\Client\bin\wswc.exe`. Zur Vereinfachung fügen Sie diesen Pfad zu Ihrer Umgebungsvariable *PATH* hinzu.

Tabelle 19-1 zeigt die Befehlszeilenoptionen, die mit dem Befehl `wswc` verwendet werden können.

Tabelle 19-1. View Client-Befehlszeilenoptionen

Option	Beschreibung
`/?`	Zeigt die Liste der Befehlsoptionen an.
`–checkin`	(Nur lokaler Desktop) Checkt den angegebenen Desktop ein und entsperrt die Online-Version. Diese Option erfordert, dass Sie auch die Option `–desktopName` festlegen.
`–checkout`	(Nur lokaler Desktop) Checkt den angegebenen Desktop aus und sperrt die Online-Version.
`–confirmRollback`	(Nur lokaler Desktop) Unterdrückt das Bestätigungsdialogfeld, das bei Verwendung der Option `–rollback` angezeigt wird. Um das Rollback im nicht interaktiven Modus auszuführen, geben Sie auch die Option `–nonInteractive` an.

Tabelle 19-1. View Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–connectUSBOnStartup`	Leitet alle gegenwärtig mit dem Host verbundenen USB-Geräte an den Desktop um. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt.
`–connectUSBOnInsert`	Verbindet ein USB-Gerät beim Anschließen des Geräts mit dem im Vordergrund angezeigten Desktop. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt.
`–desktopLayout` *Fenstergröße*	Gibt an, wie das Desktop-Fenster angezeigt wird: **`fullscreen`** Anzeige im Vollbildmodus **`multimonitor`** Anzeige auf mehreren Monitoren **`windowLarge`** Großes Fenster **`windowSmall`** Kleines Fenster
`–desktopName` *Desktop-Name*	Gibt den Namen des Desktops an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Dies ist der Anzeigename des Desktops im Dialogfeld zur Desktop-Auswahl.
`–desktopProtocol` *Protokoll*	Gibt den Namen des zu verwendenden Protokolls an, der im Dialogfeld zur Desktop-Auswahl angezeigt wird. Das Protokoll kann PCOIP oder RDP sein.
`–domainName` *Domänenname*	Gibt die Domäne an, die der Endbenutzer zur Anmeldung an View Client verwendet.
`–file` *Dateipfad*	Gibt den Pfad einer Konfigurationsdatei mit zusätzlichen Befehlsoptionen und -argumenten an. Siehe „View Client-Konfigurationsdatei“, auf Seite 427.
`–languageId` *Gebietsschema-ID*	Bietet Lokalisierungsunterstützung für verschiedene Sprachen in View Client. Wenn eine Ressourcenbibliothek verfügbar ist, geben Sie die zu verwendende Gebietsschema-ID (Locale ID, LCID) an. Für Englisch (USA) geben Sie 0x409 ein.
`–localDirectory` *Verzeichnispfad*	(Nur lokaler Desktop) Gibt an, welches Verzeichnis auf dem lokalen System zum Herunterladen des lokalen Desktops verwendet werden soll. Diese Option erfordert, dass Sie auch die Option `–desktopName` festlegen.
`–logInAsCurrentUser`	Die Anmeldeinformationen des Endbenutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View Connection Server-Instanz und schließlich an den View-Desktop übergeben.
`–nonInteractive`	Unterdrückt Fehlermeldungen beim Starten von View Client über ein Skript. Diese Option wird bei Angabe der Option `–unattended` implizit festgelegt.
`–password` *Kennwort*	Gibt das Kennwort an, das der Endbenutzer zur Anmeldung an View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn das Kennwort automatisch generiert wird.
`–printEnvironmentInfo`	Zeigt die IP-Adresse, die MAC-Adresse und den Maschinennamen des Clientgeräts an.
`–rollback`	(Nur lokaler Desktop) Entsperrt die Online-Version eines ausgecheckten Desktops und verwirft die lokale Sitzung. Diese Option erfordert, dass Sie auch die Option `–desktopName` festlegen. Um das Rollback im nicht interaktiven Modus auszuführen, geben Sie auch die Optionen `–nonInteractive` und `–confirmRollback` an.
`–serverURL` *Verbindungsserver*	Gibt die URL, die IP-Adresse oder den FQDN der View Connection Server-Instanz an.
`–smartCardPIN` *PIN*	Gibt die PIN an, wenn ein Endbenutzer eine Smartcard zur Anmeldung einführt.

Tabelle 19-1. View Client-Befehlszeilenoptionen (Fortsetzung)

Option	Beschreibung
`–unattended`	Führt View Client im nicht interaktiven Modus aus, der sich für Clients im Kiosk-Modus eignet. Zusätzlich müssen folgende Informationen angegeben werden: ■ Der Kontoname des Clients, wenn dieser nicht über die MAC-Adresse des Clientgeräts generiert wurde. Der Name muss mit der Zeichenfolge „custom-“ oder einem alternativen Präfix beginnen, das Sie in ADAM konfiguriert haben. ■ Das Kennwort des Clients, wenn dieses nicht automatisch beim Einrichten des Clientkontos generiert wurde. Über die Option `–unattended` werden die Optionen `–nonInteractive`, `–connectUSBOnStartup` und `–connectUSBOnInsert` implizit festgelegt.
`–userName` *Benutzername*	Gibt den Kontonamen an, den der Endbenutzer zur Anmeldung an View Client verwendet. Diese Option muss für Clients im Kiosk-Modus nicht angegeben werden, wenn der Kontoname über die MAC-Adresse des Clientgeräts generiert wird.

Über die Befehlszeile oder in der Konfigurationsdatei angegebene Optionen haben Vorrang vor globalen Systemrichtlinien, die wiederum Benutzerrichtlinien außer Kraft setzen.

Mit Ausnahme von `–checkin`, `–checkout`, `–file`, `–languageId`, `–localDirectory`, `–printEnvironmentInfo`, `–rollback`, `–smartCardPIN` und `–unattended` können alle Optionen über Active Directory-Gruppenrichtlinien angegeben werden.

View Client-Konfigurationsdatei

Die Befehlszeilenoptionen für View Client können einer Konfigurationsdatei entnommen werden.

Der Pfad zur Konfigurationsdatei kann als Argument der Option `–f` des `wswc`-Befehls angegeben werden. Die Datei muss als Unicode- (UTF-16) oder ASCII-Textdatei vorliegen.

Beispiel: Beispiel einer Konfigurationsdatei für eine nicht interaktive Anwendung

Das folgende Beispiel zeigt den Inhalt einer Konfigurationsdatei für eine nicht interaktive Anwendung.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Beispiel: Beispiel einer Konfigurationsdatei für einen Client im Kiosk-Modus

Das folgende Beispiel zeigt einen Client im Kiosk-Modus, dessen Kontoname auf seiner MAC-Adresse basiert. Der Client verfügt über ein automatisch generiertes Kennwort.

```
–serverURL 145.124.24.100
–unattended
```

View Client-Registrierungseinstellungen

Sie können Standardeinstellungen für View Client in der Windows-Registrierung definieren, sodass diese nicht über die Befehlszeile angegeben werden müssen.

Tabelle 19-2 zeigt die Registrierungseinstellungen für View Client. Diese Einstellungen befinden sich in der Registrierung unter `HKLM\Software\VMware, Inc.\VMware VDM\Client\`.

Richtlinieneinträge haben Vorrang vor Registrierungseinstellungen und Befehlszeileneinstellungen haben Vorrang vor Richtlinieneinstellungen.

Tabelle 19-2. View Client-Registrierungseinstellungen

Registrierungseinstellung	Beschreibung
`DomainName`	Gibt den standardmäßigen Domänennamen an.
`EnableShade`	Gibt an, ob die Menüleiste (Schatten) im oberen Bereich des View Client-Fensters aktiviert ist. Die Menüleiste ist standardmäßig aktiviert, ausgenommen für Clients im Kiosk-Modus. Bei Festlegung von **[false]** wird die Menüleiste deaktiviert.
`Password`	Gibt das standardmäßige Kennwort an.
`ServerURL`	Gibt die standardmäßige View Connection Server-Instanz über die URL, die IP-Adresse oder den FQDN an.
`UserName`	Gibt den standardmäßigen Benutzernamen an.

View Client-Exitcodes

Der Befehl `wswc` kann Exitcodes mit Informationen zu Fehlern zurückgeben, die von View Client ermittelt werden.

Tabelle 19-3 zeigt die Exitcodes, die vom Befehl `wswc` zurückgegeben werden können.

Tabelle 19-3. View Client-Exitcodes

Exitcode	Beschreibung
-1	Schwerwiegender Fehler im Kiosk-Modus.
0	Vorgang erfolgreich.
1	Verbindung fehlgeschlagen.
2	Anmeldung fehlgeschlagen.
3	Desktop konnte nicht gestartet werden.
4	RDP konnte nicht gestartet werden.
5	RDP-Vorgang fehlgeschlagen.
6	Tunnelverbindung unterbrochen.
7	Fehler beim Übertragen des lokalen Desktops.
8	Fehler beim Einchecken des lokalen Desktops.
9	Fehler beim Auschecken des lokalen Desktops.
10	Fehler beim Rollback des lokalen Desktops.
11	Unbekanntes Ergebnis während der Authentifizierung.
12	Authentifizierungsfehler.
13	Anforderung zur Verwendung einer unbekannten Authentifizierungsmethode empfangen.
14	Ungültige Serverantwort.

Tabelle 19-3. View Client-Exitcodes (Fortsetzung)

Exitcode	Beschreibung
15	Desktop wurde getrennt.
16	Tunnel wurde getrennt.
17	Für zukünftige Entwicklung reserviert.
18	Für zukünftige Entwicklung reserviert.
19	Nicht unterstützter Kiosk-Vorgang.
20	RMKS-Verbindungsfehler (Remote Mouse, Keyboard, or Screen).
21	PIN-Fehler.
22	Keine Übereinstimmung für PIN.
23	Keine Übereinstimmung für Kennwort.
24	View Connection Server-Fehler.
25	Desktop war nicht verfügbar.

Index

Symbole

.NET Framework, Migrieren des RSA-Schlüsselcontainers **354**

A

Active Directory
- Aktualisieren allgemeiner Benutzerinformationen **353**
- Aktualisieren der fremden Sicherheitsprinzipale von Benutzern **388**
- Fehlerbehebung bei verknüpften Klonen, die nicht zur Domäne hinzugefügt werden können **378**
- Vorbereiten für Clients im Kiosk-Modus **415**
- Vorbereitung für Smartcard-Authentifizierung **152**

ADM-Vorlagendatei
- Hinzufügen zu Active Directory **217**
- Hinzufügen zu einem lokalen System **216**
- installieren **216**

ADM-Vorlagendateien
- PCoIP-Sitzungsbandbreiteneinstellungen **195**
- PCoIP-Sitzungsvariablen **188**
- Speicherort **170**
- View Agent-Konfiguration **170**
- View Client-Konfiguration **174**
- View Server-Konfiguration **185**
- View-Komponenten **169**
- View-Konfiguration, allgemeine **186**

Administratorbenutzer
- erstellen **31, 32**
- Verwalten **30**

Administratorberechtigungen
- Allgemeine Verwaltung **44**
- anzeigen **34**
- Befehlszeilenprogramme **44**
- Benutzer- und Administratorverwaltung **44**
- Desktop-Verwaltung **43**
- Global **40**
- Grundlegende Informationen **27**
- häufige Aufgaben **42**
- hinzufügen **32**
- intern **42**
- löschen **33**
- objektspezifisch **41**
- persistente Festplatte, Verwaltung **43**
- Pool-Verwaltung **42**
- verwalten **32**
- vordefiniert **38**

Administratoren (Nur Lesen), Rolle **38**

Administratoren, Rolle **38**

Administratorgruppen
- entfernen **32**
- erstellen **31**
- verwalten **27**
- Verwalten **30**

Administratorrollen
- Ändern benutzerdefinierter Administratorrollen **37**
- Entfernen benutzerdefinierter Administratorrollen **37**
- Grundlegende Informationen **27**
- Hinzufügen benutzerdefinierter Administratorrollen **27, 36, 38**
- Verwalten benutzerdefinierter Administratorrollen **36**
- vordefiniert **27, 38**
- Vordefiniert **38**

Adobe Flash
- Drosselungsmodi **253**
- Festlegen von Drosselungsmodi **253**
- Festlegen von Qualitätsmodi **253**
- Qualitätsmodi **253**
- Reduzieren der Bandbreite **253**
- Terminaldienste-Sitzungen **118, 254**
- Verbessern der Qualität im Desktop **254**

Agent registrieren, Berechtigung **40**

Agent-Registrierungsadministratoren, Rolle **38**

Aktive Sitzungen
- anzeigen **255**
- neu starten **255**
- trennen **255**

Aktualisieren
- Linked-Clone-Desktops **231**
- View Composer **232**

Aktualisieren von Linked-Clone-Desktops
- Desktop-Neuzusammenstellung **233**
- Korrigieren einer nicht erfolgreichen Neuzusammenstellung **238**

Alarmeinstellungen, Leistung **186**

allowCertCRLs, Eigenschaft **159**

Anhalten der VM, Richtlinie **132**

Anmelden als aktueller Benutzer, Funktion **162**
Anpassen von Desktops, Wartungsmodus **125**
Anpassungsskripts
  Erhöhen des Limits für QuickPrep-Zeitüberschreitungen **80**
  Verwenden von QuickPrep für Linked-Clone-Desktops **100, 101**
Anpassungsspezifikationen
  erstellen **81**
  Neuzusammenstellen von Linked-Clone-Desktops **102**
Anwendungs-Repositorys
  durchsuchen **270**
  entfernen **282**
  Erstellen einer Netzwerkfreigabe **269**
  Lastausgleich **268**
  Probleme bei der Registrierung **283**
  Probleme beim Durchsuchen **283**
  registrieren **270**
Anwendungspakete
  erfassen und speichern **268**
  Erfassen und speichern **269**
ASP.NET IIS-Registrierung, Tool, RSA-Schlüsselcontainer **354**
Aufheben der Benutzerzuweisung, Dedizierte Zuweisung, Pools **256**
Aufheben der Registrierung von Desktop-Quellen **265**
Aufnahmeliste **396**
Ausgabeformate, vdmadmin, Befehl **383**
Auslagerungsdatei, Größe, Übergeordnete virtuelle Maschine **79**
Auslagerungsdateien, Linked-Clone-Desktops **75, 79**
Ausschalten der VM, Richtlinie **132**
Ausschaltskript, Anpassen von Linked-Clone-Desktops **101**
Ausschlussliste **396**
Außerkraftsetzen von IP-Adressen für View Agent **387**
Authentifizierung
  Aktivieren für Clients im Kiosk-Modus **419**
  vdmadmin, Befehl **383**
Automatische Windows-Updates, deaktivieren **71**
Automatisierte Desktop-Pools
  Ändern der Pool-Größe **249**
  Anpassen von Desktops im Wartungsmodus **125**
  Arbeitsblatt zur Erstellung **84**
  Benennen von Desktops, manuell **119, 121**
  Betriebsrichtlinien **135, 136**
  Desktop-Benennung, Beispiel **123**
  Desktop-Einstellungen **88, 126**
  erstellen **84, 87**
  Hinzufügen von Desktops, manuell **250**
  Verwenden eines Musters für die Desktop-Benennung **119**
  Wartungsmodus **125**

B

Bandbreitenreduzierung, Adobe Flash **253**
Basis-Images
  Bestimmen der Größe **302**
  Herunterladen aus dem Transfer Server-Repository **302**
Befehlsskripts, Ausführen auf Desktops **172**
Benennen von Desktop-Pools
  Beispiel **123**
  Bereitstellen eines Benennungsmusters **119**
  Manuelles Angeben von Namen **119, 121**
Benennungsmuster, Linked-Clone-Desktops **122**
Benutzer
  Aktualisieren allgemeiner Benutzerinformationen **353**
  Anzeigen nicht berechtigter Benutzer **360**
  Anzeigen von Informationen **407**
  Senden von Nachrichten **359**
Benutzerauthentifizierung, konfigurieren **145**
Benutzerdefinierte Administratorrollen
  ändern **37**
  entfernen **37**
  erstellen **27**
  verwalten **36**
Benutzerdefinierte Setup-Optionen, View Agent **49, 58**
Benutzerkonten, View Composer **15**
Benutzerpersona, Konfigurieren von Richtlinien **211**
Benutzerprofil-Repository, Richtlinien zum Erstellen **214**
Benutzerprofile
  ThinApp Sandbox-Ordner **222**
  Siehe auch Persona-Verwaltung
Benutzerprofilpfad, konfigurieren **213**
Berechtigungen
  anzeigen **29**
  einschränken **140**
  Entfernen aus Desktop-Pools **140**
  hinzufügen **32**
  Hinzufügen zu Desktop-Pools **139**
  löschen **33**
  überprüfen **140**
  Siehe auch Administratorberechtigungen
Berichte, anzeigen **390**
Bestandsliste verwalten (Nur Lesen), Berechtigung **42**
Bestandslistenadministratoren (Nur Lesen), Rolle **38**
Bestandslistenadministratoren, Rolle **38**

Betriebsrichtlinien
Automatisierte Desktop-Pools **135, 136**
Desktops und Pools **132**
Vermeiden von Konflikten **137**
Betriebssystemfestplatten
Deaktivieren von Windows 7-Diensten **66**
Desktop-Aktualisierung **231, 232**
Linked-Clone-Desktops **110**
Speichergrößen, Formeln zur Berechnung beim Bearbeiten von Pools **105, 106**
Speichermehrfachvergabe **107**
Wachstum, verursacht durch Windows 7-Dienste **67**
Bridged-Netzwerke für lokale Desktops **321**

C

certutil, Befehl **153**
Clientkonten, Hinzufügen für den Kiosk-Modus **417**
Clientsitzungen
Festlegen von Zeitüberschreitungen **18**
Globale Einstellungen **18, 19**
Zeitüberschreitung für Sitzungen **19**
Clientsitzungen, Richtlinien für
allgemein **165**
Definition **163**
Konfiguration auf Benutzerebene **165**
Konfiguration auf Pool-Ebene **164**
Konfigurieren globaler Richtlinien **164**
Lokaler **166**
Vererbung **163**
Clientsysteme
Anzeigen von Informationen zum Kiosk-Modus **401, 420**
Anzeigen von MAC-Adressen **417**
Auschecken eines Desktops nach dem manuellen Herunterladen **331**
Einrichten im Kiosk-Modus **413**
Festlegen der Standardwerte für den Kiosk-Modus **416**
Festlegen von Berechtigungen für manuell kopierte Desktop-Dateien **330**
Konfigurieren der Registrierung für die HTTP-Zwischenspeicherung **325**
Konfigurieren im Kiosk-Modus **414**
manuelles Herunterladen eines lokalen Desktops **330**
Übergabe von Informationen an Desktops **173**
Vorbereiten von Active Directory für den Kiosk-Modus **415**
CommandsToRunOnConnect, Gruppenrichtlinieneinstellung **172**
Composer-Pool-Image verwalten, Berechtigung **41**
Connection Server-Dienst **351**
crlLocation, Eigenschaft **157, 159**
CSV-Ausgabe, vdmadmin, Befehl **383**

D

Dashboard, Überwachen von View-Komponenten **349**
Data Collection Tool-Pakete, Erstellen für View Agent **361, 385**
Datei „ViewPM.adm“
Hinzufügen zu Active Directory **217**
Hinzufügen zu einem lokalen System **216**
Datenbankwiederherstellung, View Composer, sviconfig **347**
Datenspeicher
Größenrichtlinien für Linked-Clone-Pools **102**
Speichergröße, Tabelle zur **103**
Speichern von verknüpften Klonen und Replikaten **109**
DCT-Pakete, Erstellen für View Agent **361, 385**
Dedizierte Zuweisung, Pools
Auswahl eines Typs für die Benutzerzuweisung **119**
Besitzrechte **391**
Entfernen von Benutzerzuweisungen **256**
Wartungsmodus **125**
Zuweisen von Besitzrechten **255**
Deduplizierung
Auswirkung auf Datenübertragungen **316**
Datenübertragungen für lokale Desktops **313**
Defragmentierung, Deaktivierung auf verknüpften Klonen **70**
Delegieren der Verwaltung **28**
Deltafestplatten, Speichermehrfachvergabe **108**
Desktop-Aktualisierung, Verknüpfte Klone **232**
Desktop-Benutzeroberfläche, Gruppenrichtlinieneinstellungen **229**
Desktop-Einstellungen
Automatisierte Desktop-Pools **88, 126**
Linked-Clone-Desktops **97**
Manuelle Desktop-Pools **115, 126**
Terminalserver-Desktop-Pools **117, 126**
Desktop-Neuzusammenstellung
Korrigieren einer nicht erfolgreichen Neuzusammenstellung **238**
Linked-Clone-Desktops **233, 234, 237**
Sysprep **102**
Vorbereiten einer übergeordneten virtuellen Maschine **234**
Desktop-Pool-Erstellung
Anpassen im Wartungsmodus **125**
Auswahl eines Typs für die Benutzerzuweisung **119**
Bereitstellungsoptionen **118**
Desktop-Benennung, Beispiel **123**

Grundlegende Informationen **83**
mit Persona-Verwaltung **220**
Desktop-Pool-Verwaltung
Bearbeitbare Desktop-Pool-Einstellungen **248**
Bearbeiten von Desktop-Pools **247**
Deaktivieren der Bereitstellung **251**
Deaktivieren von Desktop-Pools **251**
Feste Desktop-Pool-Einstellungen **248**
Grundlegende Informationen **247**
Löschen nicht verwalteter Desktops **264**
Löschen von Desktop-Pools **252**
Desktop-Pool, Fehlerbehebung
Anmelden an vCenter nicht möglich **371**
Anpassungsfehler **373**
Erstellungsprobleme **370**
Fehler aufgrund der Überlastung von vCenter **372**
Fehler aufgrund von Berechtigungsproblemen **370**
Fehler aufgrund von fehlenden Anpassungsspezifikationen **370**
Fehler aufgrund von Konfigurationsproblemen **371**
Klonfehler **372**
Ressourcenprobleme **372**
Speicherplatzprobleme **372**
vCenter-Status unbekannt **371**
Virtuelle Maschinen verlassen den Bereitstellungsstatus nicht **373**
Zeitüberschreitung während der Anpassung **372**
Desktop-Quellen
Aufheben der Registrierung **265**
Entfernen aus einem Pool **264**
Hinzufügen zu einem Pool **263**
Vorbereiten für die Desktop-Bereitstellung **51**
Desktop-Sitzungen
anzeigen **255**
neu starten **255**
trennen **255**
Desktop-Status
Physische Computer **265**
Suchen nach Desktops **257, 349**
Terminalserver **265**
Virtuelle Maschinen **258**
Desktop-Verwaltung
Anzeigen des ersten Benutzers eines Desktops **405**
Anzeigen von Desktops für nicht berechtigte Benutzer **400**
Exportieren von Desktop-Informationen in eine Datei **260**
Grundlegende Informationen **255**
Löschen von Desktops **259**
Überwachen des Desktop-Status **257, 349**
Desktop, Fehlerbehebung
Anzeigen von problematischen Desktops **359**
Anzeigen von verwaisten Desktops **360**
Verbindungsprobleme **368**
DFÜ-Netzwerkverbindung, Auschecken lokaler Desktops **328**
Diagnoseinformationen
sammeln **361**
Sammeln für View Composer **362**
Sammeln mithilfe des Supporttools **363**
Verwenden von Supportskripts **364**
Diagnoserichtliniendienst, deaktivieren **72**
Dienste
Grundlegende Informationen **350**
Sicherheitsserver, Hosts **351**
starten und beenden **350**
View Connection Server-Hosts **351**
View Transfer Server-Hosts **352**
Direkte Interaktion, Berechtigung **40**
Direkte Verbindungen
konfigurieren **21**
Lokale Desktops **314**
Domänen
Auflisten vertrauenswürdiger Domänen **185**
Filterlisten **393**
Domänenfilter
Anzeigen **393**
Beispiel für das Ausschließen von Domänen **398**
Beispiel für das Einschließen von Domänen **397**
konfigurieren **396**
Drittanbieteranwendungen, Unterstützung in View Composer **98**
Drucken, standortbasiert **200**
Dynamische Zuweisung, Pools
Auswahl eines Typs für die Benutzerzuweisung **119**
Wartungsmodus **125**

E

E/A-Vorgänge pro Sekunde, Vorteile der Deaktivierung von Windows 7-Diensten **66**
Eingeschränkte Berechtigungen
Beispiele **141**
Einschränkungen **143**
Grundlegende Informationen **140**
Kennzeichenabgleich **142**
konfigurieren **143**
Zuweisen von Kennzeichen zu Desktop-Pools **144**
Einmalige Anmeldung (Single Sign-On, SSO)
Aktivieren für lokale Desktop-Vorgänge **19**

Festlegen eines Zeitlimits **22**
Gruppenrichtlinieneinstellungen **170, 174**
Einstellung des Speicherorts für das Persona-Repository, konfigurieren **218**
Einstellung zum Verwalten von Benutzerpersona, konfigurieren **218**
Einzelne Desktops, erstellen **113**
empfohlene Vorgehensweisen, View Persona-Verwaltung **220**
enableOCSP, Eigenschaft **158, 159**
enableRevocationChecking, Eigenschaft **157–159**
Endpunkte, Ressourcennutzung, konfigurieren **318**
Enterprise NTAuth-Speicher, Hinzufügen von Stammzertifikaten **153**
Entsperrung
Remote-Desktops **409**
View Transfer Server-Instanzen **409**
Ereignisse
Typen und Beschreibungen **359**
überwachen **358**
Ergebniscodes, restoredata-Operation **348**
Ermitteln von Konflikten bei LDAP-Einträgen **410**
externe URL, Bearbeiten **24**

F

Filterlisten, Hinzufügen und Entfernen von Domänen **393**
Flexible Authentifizierung **413**
Framework-Komponente, Dienst **351**
Fremde Sicherheitsprinzipale, aktualisieren **388**
FSPs, aktualisieren **388**

G

Gastbetriebssysteme
Auslagerungsdatei, Größe **79**
Dateisystemoptimierung **318**
installieren **54**
Optimieren der Leistung **65, 66**
Vorbereiten für die Desktop-Bereitstellung **55**
Getrennte persistente Festplatten
Bearbeiten von Pool oder Benutzer **243**
löschen **245**
Neuerstellung eines Desktops **244**
verknüpfen **242**
Gewähren von Berechtigungen für Pools, Berechtigung **41**
GINA
Verkettung von Drittanbieter-Software-dlls **378**
View Agent dll **378**
Globale Einstellungen
Clientsitzungen **18, 19**
Sicherheitsmodus für Nachrichten **20**
Globale Konfiguration und Richtlinien verwalten (Nur Lesen), Berechtigung **42**
Globale Konfiguration und Richtlinien verwalten, Berechtigung **40**
Globale Konfiguration und Richtlinienadministratoren (Nur Lesen), Rolle **38**
Globale Konfiguration und Richtlinienadministratoren, Rolle **38**
Globale Richtlinien, konfigurieren **164**
Glossar **7**
GPOs
Erstellen für Desktops **207**
Erstellen für View-Komponentenrichtlinien **168**
Grafiken, Windows 7-3D-Rendering **131**
Gruppenrichtlinien
ADM-Vorlagendateien **170**
Anwenden auf GPOs **207**
Beispiele **205**
Terminaldienste **204, 205**
View Agent-Konfiguration **170**
View Client-Konfiguration **174**
View Connection Server **185**
View-Komponenten **169**
View-Konfiguration, allgemeine **186**
Gruppenrichtlinieneinstellungen
Desktop-Benutzeroberflächeneinstellungen **229**
Hinzufügen zu Active Directory **217**
Hinzufügen zu einem lokalen System **216**
konfigurieren **218**
Ordnerumleitung **227**
Protokollieren **229**
Serverspeicherung und Synchronisierung **225**
Speicherort für das Persona-Repository **225**
Verwalten von Benutzerpersona **225**
View Persona-Verwaltung **223**
GUIDs
Anzeigen für View Connection Server-Gruppen **388**
Unterstützung in View Composer **98**

H

HTTP-Cache
Bereitstellen lokaler Desktops **323**
Konfigurieren eines Proxy-Servers **326**
Konfigurieren von Clientsystemen **325**
Konfigurieren von View Connection Server **323**
Konfigurieren von View LDAP **324**

I

Immer eingeschaltet, Richtlinie **132**
Informationen, Anmeldung **162**

Installation
Gastbetriebssystem **54**
unbeaufsichtigt **59**
Unbeaufsichtigte Installation, Optionen **60**
View Agent **48, 57, 59**
IP-Adressen
Außerkraftsetzen für View Agent **387**
Fehlerbehebung bei Linked-Cloned-Desktop-Verbindungen **369**

K

Keine Aktion, Richtlinie **132**
keyfile, Eigenschaft **355**
keypass, Eigenschaft **355**
keytool, Dienstprogramm **148**
Kiosk-Modus
Aktivieren der Authentifizierung von Clients **419**
Anzeigen der MAC-Adresse von Clientgeräten **417**
Anzeigen und Ändern von Clientkonten **401**
Anzeigen von Informationen zu Clients **420**
einrichten **413**
Festlegen der Standardwerte für Clients **416**
Hinzufügen von Clientkonten **417**
konfigurieren **414**
Verbinden mit Desktops **421**
Verwalten der Clientauthentifizierung **401**
Vorbereiten von Active Directory **415**
KMS-Lizenzschlüssel, Volumenaktivierung auf verknüpften Klonen **77**
Knowledge Base-Artikel, Website **365**
Komprimierung
Auswirkung auf Datenübertragungen **316**
Datenübertragungen für lokale Desktops **313**
Konfigurationsdaten
Export mit vdmexport **345**
Import mit vdmimport **346**
Konsoleninteraktion, Berechtigung **40**

L

Lastausgleich, Anwendungs-Repositorys **268**
LDAP-Einträge, Ermitteln und Lösen von Konflikten **410**
LDAP-Repository
importieren **346**
Sicherung **345**
Leistungsalarme, konfigurieren **186**
Leistungsoptimierung, Gastbetriebssystem **65, 66**
Linked-Clone-Desktop-Verwaltung, Neuzusammenstellung **234**
Linked-Clone-Desktop, Erstellung
anpassen **99**
Arbeitsblatt zur Erstellung **89**
Auswahl von QuickPrep oder Sysprep **99**
Auswählen eines Benennungsmusters **122**
Datenfestplatten, Erstellung **110**
Desktop-Einstellungen **97**
Festlegen des Grads der Speichermehrfachvergabe **107**
Grundlegende Informationen **89**
Speichergröße, Tabelle zur **103, 105**
Speichergrößen **102**
Speichermehrfachvergabe, Funktion **108**
Speichern von Auslagerungsdateien **75, 79**
Speichern von Replikaten und verknüpften Klonen in separaten Datenspeichern **109**
Unterstützung für eindeutige SIDs **98**
Verwendung von View Composer **96**
Windows 7- und Vista-Volumenaktivierung **77**
Linked-Clone-Desktops, Fehlerbehebung
Bereitstellungsfehlercodes **376**
Korrigieren einer nicht erfolgreichen Neuzusammenstellung **238**
Verbindungsprobleme **369**
Windows XP-Desktops, Fehler beim Hinzufügen zu Domäne **378**
Linked-Clone-Desktops, Verwaltung
Aktualisieren **231**
Aktualisierungen, Richtlinien **232**
Festplattendateinamen nach einer Neuverteilung **241**
Grundlegende Informationen **231**
Neuverteilung **238, 240**
Neuzusammenstellung **237**
Neuzusammenstellung von Desktops **233**
Trennen persistenter Festplatten **242**
Verwalten persistenter Festplatten **241**
Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung **234**
Wiederherstellen persistenter Festplatten aus vSphere **244**
Linux-Systeme, Verwendung mit View Administrator **12**
Lizenzen, Hinzufügen zu VMware View **352**
locked.properties, Datei
Konfigurieren der OCSP-Überprüfung **158**
Konfigurieren der Smartcard-Authentifizierung **149**
Konfigurieren der Smartcard-Zertifikatssperrüberprüfung **159**
Konfigurieren der Überprüfung von Zertifikatssperrlisten **157**
Log in as current user feature (Anmelden als aktueller Benutzer, Funktion), Gruppenrichtlinieneinstellungen **174**

Lokale Arbeitsspeichernutzung, Außerkraftsetzung **318**
Lokale CPU-Nutzung, Außerkraftsetzung **318**
Lokale Desktops, Fehlerbehebung **332**
Lokale Sitzungen
anzeigen **358**
Berechtigungen zum Verwalten **41, 43**
Rollback **311, 409**
Lokale Sitzungen verwalten, Berechtigung **41**
Lokaler Datenspeicher, Linked-Clone-Desktops, Auslagerungsdateien **75, 79**
Lokaler Desktop, Konfiguration
Aktivieren von SSO **19**
Ändern des Netzwerktyps in Bridged **321**
Bereitstellen mithilfe eines HTTP-Caches **323**
Datenübertragung, Deduplizierungs- und Komprimierungseinstellungen **313**
Einstellungen der Sicherheitsoptionen **314**
empfohlene Vorgehensweisen **295**
Erstellung und Bereitstellung, Übersicht **292**
Festlegen von Replikationsrichtlinien **309**
Festlegen, dass ein Desktop ausschließlich im lokalen Modus ausgeführt werden kann **293**
Grundlegendes zu Datenübertragungsrichtlinien **309**
Grundlegendes zum Taktsignalintervall **327**
Grundlegendes zum Transfer Server-Repository **302**
Hinzufügen einer View Transfer Server-Instanz **297**
Konfigurieren der Verschlüsselungsmethode **315, 316, 334**
Konfigurieren der Zwischenspeicherung von Basis-Images auf einem Proxy-Server **326**
Konfigurieren des Taktsignalintervalls für alle Clientcomputer **327**
Konfigurieren des Taktsignalintervalls für einen Clientcomputer **328**
Konfigurieren von Clientsystemen für die Verwendung eines zur Zwischenspeicherung eingesetzten Proxy-Servers **325**
Konfigurieren von SSL für lokale Desktop-Vorgänge **313**
Optimieren von Datenübertragungen **313**
Reparieren einer virtuellen Festplatte **339**
Richtlinieneinstellungen **166**
Lokaler Desktop, Verwaltung
Anhalten von Datenübertragungen **299**
Authentifizierungsverzögerungen **334**
Entfernen einer View Transfer Server-Instanz **298**
Festlegen von Berechtigungen für manuell kopierte Desktop-Dateien **330**
Grundlegendes zu Managementaufgaben **289**
Initiieren einer Replikation **310**
Kopieren von Paketdateien auf ein tragbares Gerät **329**
manuelles Herunterladen von Desktops **328**
manuelles Kopieren von Desktop-Dateien **330**
Neuzusammenstellung eingecheckter Desktops **236**
Rollback eines ausgecheckten Desktops **311**
Sperrung und Entsperrung von Remote-Desktops **409**
Verbessern der Datenübertragungsleistung **300**
Wiederherstellen von Daten aus virtuellen Maschinen **339, 408**
Lokaler Desktop, Verwendung
Anmelden über Smartcards **146**
auschecken **294**
Auschecken nach dem manuellen Herunterladen **331**
Löschen lokaler Desktops **312**
Rollback eines ausgecheckten Desktops **311**
Vorteile **289**
lokaler Modus, *, siehe* lokaler Desktop
Lokaler Modus, als einzigen Modus für Desktops festlegen **293**
Lokaler Modus, Richtlinien **166**
Loopback-Verarbeitung
aktivieren **208**
Vorteile **169**
Löschbare Dateien, Umleitung, Auslagerungsdatei, Größe **79**
Löschbare Daten, Festplatten für, Linked-Clone-Desktops **110**
Lösen von Konflikten bei LDAP-Einträgen **410**
LSI20320-R-Controller, Installieren des Treibers **54**

M

MAC-Adressen, Anzeigen für Clientsysteme **417**
Mac-Systeme, Verwendung mit View Administrator **12**
Manuelle Desktop-Pools
Arbeitsblatt zur Erstellung **111**
Desktop-Einstellungen **115, 126**
erstellen **111, 113**
Konfigurieren eines einzelnen Desktops **113**
Maussteuerung in Desktop-Fenster **294**
Maximale Dateigröße zur Unterteilung von Paketen, Anzeigen und Festlegen für View Transfer Server **407**
Mehrere Netzwerkkarten, Konfigurieren für View Agent **64**

Microsoft Windows Defender, Deaktivieren unter Windows 7 **74**
Microsoft Windows Installer, Eigenschaften für View Agent **62**
Microsoft-Feeds-Synchronisierung, Deaktivieren unter Windows 7 **74**
Microsoft-Terminaldienste, Erstellen von Desktop-Pools **116**
Microsoft-Terminaldienste-Pools
  Adobe Flash-Drosselung **118, 254**
  erstellen **117**
MSI-Pakete
  erstellen **268, 269**
  ungültig **286**

N

Nach Synchronisierung ausgeführtes Skript, Anpassen von Linked-Clone-Desktops **101**
Nachrichten, Senden an Desktop-Benutzer **359**
Nachrichtenbuskomponente, Dienst **351**
NAT bei lokalen Desktops **321**
Netzwerkfreigabe, Richtlinien zum Erstellen **214**
Netzwerkkarten **321**
Netzwerkverbindungen
  Fehlerbehebung **365**
  Manuelles Herunterladen von Desktops **328**
Neustart verwalten, Berechtigung **41**
Neuverteilung von Linked-Clone-Desktops, Festplattendateinamen nach einer Neuverteilung **241**
Neuzusammenstellen von Linked-Clone-Desktops, Sysprep **102**
Neuzusammenstellung von Desktops
  Korrigieren einer nicht erfolgreichen Neuzusammenstellung **238**
  Lokale Desktops **236**
  View Composer **233, 237**
Nicht berechtigte Benutzer
  anzeigen **360**
  Anzeigen von Desktops **400**
Nicht verwaltete Desktop-Quellen
  Aufheben der Registrierung **265**
  Definition **47**
  Entfernen aus einem Pool **264**
  Hinzufügen zu einem Pool **263**
  Installieren von View Agent **48**
  Vorbereiten für die Desktop-Bereitstellung **47**
Nicht zusammenhängende Namespaces **267**
NTFS, Optimieren von Datenübertragungen **318**

O

OCSP-Zertifikatssperrüberprüfung
  anmelden **157**
  Konfigurieren **158**
ocspCRLFailover, Eigenschaft **159**
ocspSendNonce, Eigenschaft **159**
ocspSigningCert **159**
ocspSigningCert, Eigenschaft **158**
ocspURL, Eigenschaft **158, 159**
Offline Desktop (Local Mode), *, siehe* lokaler Desktop
Offline-Smartcard-Authentifizierung **146**
Online-Support **7**
Ordner
  entfernen **35**
  erstellen **28, 29, 35**
  Hinzufügen eines Desktop-Pools **35**
  Organisieren von Desktops und Pools **28**
  Stammordner **28**
  Überprüfen von Desktop-Pools **36**
  Überprüfen von Desktops **36**
  verwalten **34**
Ordnerumleitung, Gruppenrichtlinieneinstellungen **227**
OUs
  Erstellen für Clients im Kiosk-Modus **415**
  Erstellen für View-Desktops **169, 206**

P

Paketdateien
  Kopieren auf ein tragbares Gerät **329**
  Löschen aus dem Transfer Server-Repository **305**
  Veröffentlichen im Transfer Server-Repository **305**
Pakete, Anzeigen und Festlegen der maximalen Dateigröße **407**
PCoIP Server (PCoIP-Server), View Agent, benutzerdefinierte Option **49, 58**
PCoIP Smartcard (PCoIP-Smartcard), View Agent, benutzerdefinierte Option **49, 58**
PCoIP-Sitzungsvariablen
  Allgemeine PCoIP-Sitzungsvariablen **189**
  Build-to-Lossless-Funktion **199**
  Gruppenrichtlinieneinstellungen **188**
  Sitzungsbandbreiteneinstellungen **195**
  Tastatureinstellungen **198**
pcoip.adm, ADM-Vorlagendateien **170**
Persistente Festplatten
  Bearbeiten von Pool oder Benutzer **243**
  erstellen **89**
  Grundlegende Informationen **241**
  Importieren aus einem vSphere-Datenspeicher **244**
  Linked-Clone-Desktops **110**
  Löschen getrennter Festplatten **245**
  Neuerstellung eines Desktops **244**
  Persona-Verwaltung **223**
  Speichergrößen, Formeln zur Berechnung beim Bearbeiten von Pools **105, 106**

trennen **242**
verknüpfen **242**
View Composer **241**
Persistente Festplatten verwalten, Berechtigung **41**
Persona-Verwaltung
empfohlene Vorgehensweisen **220**
Erstellen von Desktop-Pools **220**
Konfigurationsübersicht **212**
Konfigurieren einer Bereitstellung **212**
Konfigurieren und Verwalten **211**
mit View Manager **211**
Servergespeicherte Windows-Profile **212**
View Agent-Installationsoption **214**
View Composer, persistente Festplatten **223**
Physische Computer
Anzeigen von Informationen **392**
Desktop-Status **265**
Entfernen aus einem Pool **264**
Hinzufügen zu einem Pool **263**
Installieren von View Agent **48**
verwalten **263**
Vorbereiten für die Desktop-Bereitstellung **47**
Pool aktivieren, Berechtigung **41**
Pool verwalten, Berechtigung **41**
Pool-Größe, ändern **249**
Prä-Anmeldenachrichten, Anzeige auf Clients **19**
Problematische Desktops, anzeigen **358, 359**
Professional Services **7**
Protokolldateien
Anzeigen für View Connection Server **155**
Konfigurieren in View Agent **385**
Konfigurieren von Einstellungen **186**
Sammeln für View Client **362**
Protokollieren, Gruppenrichtlinieneinstellungen **229**
Protokollierungsebenen, View Agent **385**
Proxy-Caches, Festlegen einer maximalen Dateigröße zur Unterteilung von Paketen für View Transfer Server **407**
proxy.pac-Dateien, Konfigurieren von View Client zur Verwendung von **174**

Q

QuickPrep
Anpassungsfehler **376**
Anpassungsskripts **100, 101**
Erhöhen des Zeitüberschreitungslimits für Anpassungsskripts **80**
Fehlerbehebung bei Anpassungsfehlern **375**
View Composer **99, 100**

R

RDP, Zugriff auf Desktops deaktivieren **131**
Registrierung
Einstellungen für den wswc-Befehl **428**
Einstellungen für View Client **428**
Registrierungssicherung (RegIdleBackup), deaktivieren **73**
Remote-Desktop-Benutzer, Gruppe **55**
Remote-Desktop-Verbindungen
aktivieren **55**
RDP deaktivieren **131**
Remote-Desktops
abmelden **294**
Benutzer-initiiertes Rollback, Einstellung **166**
Erstellen **297**
Festlegen von Replikationsrichtlinien **309**
Konfigurieren einer sicheren Tunnelverbindung **314**
Sperrung und Entsperrung **409**
USB-Umleitungsprobleme **373**
Vergleich mit lokalen Desktops **289**
Remote-Repository, konfigurieren **213**
Remote-Sitzungen
anzeigen **358**
Berechtigungen zum Verwalten **41, 43**
Remote-Sitzungen verwalten, Berechtigung **41**
Replikation
Deduplizierung und Komprimierung **313**
Initiieren einer Anforderung **310**
Konfigurieren von Richtlinien **309**
restoredata, Ergebniscodes **348**
Richtlinien
Active Directory **168**
allgemein, für Clientsitzung **165**
Anzeigen für nicht berechtigte Benutzer **400**
Anzeigen nicht berechtigter Benutzer **360**
Automatisierte Pools **135**
Benutzerebene **165**
Betriebsrichtlinien **132, 135**
Clientsitzung, Vererbung **163**
Clientsitzungen **163**
global **164**
Konfigurieren für View **163**
Konfigurieren von Persona-Verwaltung **211**
Lokaler Modus **166**
Pool-Ebene **164**
Vertrauenswürdige Stammzertifizierungsstellen **153**
Zwischenzertifizierungsstellen **154**
Rollen, *, siehe* Administratorrollen
Rollen und Berechtigungen verwalten, Berechtigung **40**

Rollenbasierte Verwaltungsdelegierung
empfohlene Vorgehensweisen **45**
konfigurieren **27**
RSA SecurID-Authentifizierung
aktivieren **160**
Anmeldung **160**
konfigurieren **159**
RSA-Agentenhost-Knotenkennwort, zurücksetzen **161**
RSA-Schlüsselcontainer
Migrieren auf View Composer **353, 354**
Verwendung von .NET Framework **354**

S

Schreibgeschützte Domänencontroller, Fehlerbehebung bei verknüpften Klonen, die nicht zur Domäne hinzugefügt werden können **378**
Schulungsressourcen **7**
SCOM, Festlegen des Namens einer View Connection Server-Gruppe **388**
Senden von Nachrichten an Desktop-Benutzer **359**
servergespeicherte Profile, *, siehe* Persona-Verwaltung
Servergespeicherte Windows-Profile, Persona-Verwaltung **212**
Serverspeicherung und Synchronisierung, Gruppenrichtlinieneinstellungen **225**
Setup Capture-Assistent, ThinApp **268**
sicheres PCoIP-Gateway, Verbindungsprobleme **367**
Sicherheits-Gateway-Komponente, Dienst **351**
Sicherheitseinstellungen, Gruppenrichtlinie **174**
Sicherheitsmodus für Nachrichten, Globale Einstellungen **20**
Sicherheitsserver
Aktivieren der Smartcard-Authentifizierung **149**
Aktualisieren von Zertifikaten **355**
Dienste **351**
Eingeschränkte Berechtigungen, Einschränkungen **143**
Verbindungsprobleme mit dem sicheren PCoIP-Gateway **367**
Sicherheitsserver, Dienst **351**
Sicherung
Konfigurationssicherung, Einstellungen **345**
Planen von Sicherungen **344**
View Connection Server **18**
View-Konfigurationsdaten **343**
SIDs, Unterstützung in View Composer **98**
Sitzungen
anzeigen **255**
neu starten **255**
trennen **255**
Skripthost, Dienst **351**
Smartcard-Authentifizierung
Active Directory-Vorbereitung **152**
Aktivieren von SSO **174**
Benutzerprinzipalnamen (UPNs) für Smartcard-Benutzer **152**
Grundlegende Informationen **145**
konfigurieren **146, 149, 150**
Offline-Smartcard-Authentifizierung **146**
Überprüfen der Konfiguration **155**
Umleiten von Karten und Leser **174**
Zertifikatssperrüberprüfung **156**
Smartcard-Zertifikate, sperren **156**
Smartcards
Exportieren von Benutzerzertifikaten **148**
Verwenden zur Authentifizierung **146**
Verwendung mit lokalen Desktops **146**
Solid-State-Disks, Speichern von View Composer-Replikaten **109**
Speichermehrfachvergabe
verknüpfte Klone **107**
Verknüpfte Klone **108**
Speicherort für das Persona-Repository, Gruppenrichtlinieneinstellungen **225**
Sperrung
Remote-Desktops **409**
View Transfer Server-Instanzen **409**
SSL
Aktivieren für Clientverbindungen **18, 19**
Lokaler Desktop, Vorgänge **313, 314**
SSL-Zertifikate, *, siehe* Zertifikate
SSO (Single Sign-On)
Aktivieren für Offline-Desktop-Vorgänge **19**
Festlegen eines Zeitlimits **22**
Gruppenrichtlinieneinstellungen **170, 174**
Stammordner **28**
Stammzertifikate
anfordern **147**
exportieren **148**
Hinzufügen zu vertrauenswürdigen Stammzertifizierungsstellen **153**
Hinzufügen zum Enterprise NTAuth-Speicher **153**
Importieren in eine Server-Vertrauensspeicherdatei **148**
Standortbasierter Druck
Gruppenrichtlinie **200–202**
konfigurieren **200**
Registrierungsschlüssel **200**
TPVMGPoACmap.dll, Datei **201**
storetype, Eigenschaft **355**
Strg+Alt zur Freigabe des Mauszeigers **294**
Suche, Ausschlussliste **396**

Supportanfragen
aktualisieren **365**
Sammeln von Protokolldateien **362**
Supportangebote **7**
Supportskripts
Sammeln von Diagnoseinformationen **364**
View Composer **362**
Supporttool, Verwenden zum Sammeln von Diagnoseinformationen **363**
sviconfig-Dienstprogramm
Ergebniscodes für restoredata **348**
Wiederherstellen der Datenbank **347**
Sysprep
Linked-Clone-Desktops **99**
Neuzusammenstellen von Linked-Clone-Desktops **102**
Systemüberwachungen, auflisten und anzeigen **389**
Systemwiederherstellung, deaktivieren **73**
Systemzustand, Dashboard **358**

T

Taktsignalintervall
lokale Desktops **327**
Lokale Desktops **327, 328**
Tastatureinstellungen, PCoIP-Sitzungsvariablen **198**
Technischer Support, Ressourcen **7**
Terminaldienste-Gruppenrichtlinien **204, 205**
Terminalserver
Desktop-Status **265**
Installieren von View Agent **48**
verwalten **263**
Vorbereiten für die Desktop-Bereitstellung **47**
Terminalserver-Desktop-Pools
Desktop-Einstellungen **117, 126**
erstellen **116**
Textanzeigeprobleme, View Administrator **12**
ThinApp Setup Capture-Assistent **268**
ThinApp-Anwendungen
aktualisieren **279**
Anforderungen **267**
Anzeigen von MSI-Paketinformationen **279**
Anzeigen von Zuweisungen **277**
Entfernen aus View Administrator **281**
Entfernen von Zuweisungen **280, 281**
Fehlerbehebung **282**
Konfigurationsbeispiel **286**
Konfigurieren von Benutzerprofilen **222**
paketieren **269**
Probleme bei der Deinstallation **285**
Probleme bei der Installation **284**
Probleme bei der Zuweisung **284**
Überprüfen des Installationsstatus **278**
warten **279**
zuweisen **272–276**
ThinApp-Vorlagen
entfernen **282**
erstellen **271**
zuweisen **276**
TPVMGPoACmap.dll, Datei **201**
Transfer Server-Dienst **352**
Transfer Server-Repository
Bestimmen der Größe eines Basis-Images **302**
Herunterladen der System-Images **302**
konfigurieren **303**
Kopieren von Paketen auf ein tragbares Gerät **329**
Löschen eines Pakets **305**
migrieren **306**
neu erstellen **308**
Statuswerte **300**
Veröffentlichen eines Pakets **305**
verwalten **302**
Wiederherstellen eines beschädigten freigegebenen Ordners **308**
Transfer Server-Steuerungsdienst **352**
Treiber, installierte Treiber auf Clientsystemen für lokale Desktops **294**
trustKeyfile, Eigenschaft **149**
trustStoretype, Eigenschaft **149**
Tunnelverbindungen, Lokale Desktops **314**

U

Übergeordnete virtuelle Maschinen
Deaktivieren der Defragmentierung unter Windows 7 **70**
Deaktivieren des Ruhezustands **78**
Deaktivieren von Windows 7-Diensten **66**
Vorbereiten für View Composer **75**
Uhrzeitsynchronisierung
Desktop und Clientsystem **174**
Gastbetriebssystem und ESX-Host **55**
Unbeaufsichtigte Installation, View Agent **59**
Unbeaufsichtigte Installation, Optionen **60**
Unbekannter Benutzername oder falsches Kennwort **401, 419**
Unix-Systeme, Verwendung mit View Administrator **12**
Update-Dienst, deaktivieren **71**
UPHClean-Dienst, Verwenden mit Persona-Verwaltung **215**
UPNs, Smartcard-Benutzer **152**
USB-Geräte, Gruppenrichtlinieneinstellungen **174**
USB-Umleitung
Fehlerbehebung **373**
Konfigurieren in View Agent **49, 58**

useCertAuth, Eigenschaft **149, 155**
userPrincipalName, Attribut **152**

V

vCenter Server-Instanzen
- Entfernen aus View Administrator **14**
- Hinzufügen in View Administrator **12, 13**
- Korrigieren von Konflikten bei eindeutigen IDs **17**

vdm_agent.adm **170**
vdm_client.adm **170, 174**
vdm_common.adm **170, 186**
vdm_server.adm **170, 185**
vdmadmin, Befehl
- Ausgabeformate **383**
- Authentifizierung **383**
- Befehlsoptionen **384**
- Einführung **381**
- Syntax **383**

Verbindungen, Fehlerbehebung **365**
Verbindungsprobleme
- Linked-Clone-Desktops mit statischen IP-Adressen **369**
- View Client und sicheres PCoIP-Gateway **367**
- zwischen Desktops und View Connection Server **368**
- zwischen View Client und View Connection Server **365**

Verbindungsticket, Zeitüberschreitung **170**
Verschlüsselung, Anmeldeinformationen **162**
Vertrauenswürdige Domänen, auflisten **185**
Vertrauenswürdige Stammzertifizierungsstellen, Richtlinie **153**
Verwaiste Desktops, anzeigen **360, 400**
Verwalten von Benutzerpersona, Gruppenrichtlinieneinstellungen **225**
Verwaltung
- delegieren **28**
- konfigurieren **27**

View Administrator
- Anmeldung **10**
- Fehlerbehebung für die Anmelde-URL **12**
- Navigation **10**
- Textanzeigeprobleme **12**
- Tipps zur Verwendung **10**
- Übersicht **9**
- Verwalten einer View-Bereitstellung **9**
- Verwenden des Dashboards zum Systemzustand **358**
- Verwendung mit Linux, Unix oder Mac **12**

View Agent
- Außerkraftsetzen von IP-Adressen **387**
- Benutzerdefinierte Setup-Optionen **49, 58**
- Erstellen eines Data Collection Tool-Pakets **361**
- Installieren auf einer virtuellen Maschine **57**
- Installieren auf nicht verwalteten Desktop-Quellen **48**
- Konfigurieren mehrerer Netzwerkkarten **64**
- Konfigurieren von Protokollierungsebenen **385**
- mit View Persona-Verwaltung **214**
- Sammeln von Diagnoseinformationen **364**
- Unbeaufsichtigte Installation **59**
- Unbeaufsichtigte Installation, Eigenschaften **62**

View Client
- Ausführen über die Befehlszeile **425**
- Befehlssyntax **425**
- Fehlerbehebung **357**
- Fehlerbehebung bei der USB-Umleitung **373**
- Fehlerbehebung bei Verbindungsproblemen **365**
- Konfigurationsdatei **427**
- Konfigurieren des Online-Hilfe-URLs **174**
- Registrierungseinstellungen **428**
- Sammeln von Diagnoseinformationen **364**
- Speichern von Protokolldateien **362**
- Verbessern der Adobe Flash-Qualität **254**
- Verbindungsprobleme mit dem sicheren PCoIP-Gateway **367**
- Verwenden mit Kiosk-Clients **421**

View Client with Local Mode verwenden, *, siehe* lokaler Desktop
View Composer Agent
- View Agent, benutzerdefinierte Option **58**
- View Agent, benutzerdefinierte Setup-Option **58**

View Composer-Konfiguration
- Entfernen des Dienstes aus vCenter Server **16**
- Erstellen eines Benutzerkontos **15**
- Konfigurieren von Einstellungen für vCenter Server **15**
- Löschen von Basis-Images **305**
- Unterstützung für eindeutige SIDs **98**
- Veröffentlichen von Basis-Images **302**
- Volumenaktivierung **77**

View Composer-Wartung
- Migrieren des Dienstes auf einen anderen Computer **353**
- Migrieren eines RSA-Schlüsselcontainers **354**
- Planen von Sicherungen **344**
- Sichern von Konfigurationsdaten **18, 343**
- Wiederherstellen der Datenbank **347**
- Wiederherstellen von Konfigurationsdaten **346**

View Composer, Fehlerbehebung
Bereitstellungsfehlercodes **376**
Korrigieren einer nicht erfolgreichen Neuzusammenstellung **238**
QuickPrep-Skriptfehler **375**
Sammeln von Diagnoseinformationen **362**
Übersicht **357**
View Composer, persistente Festplatten
Bearbeiten von Pool oder Benutzer **243**
Grundlegende Informationen **241**
Importieren aus vSphere **244**
Löschen getrennter Festplatten **245**
Speichergrößen, Formeln zur Berechnung beim Bearbeiten von Pools **106**
Speichergrößen, Formeln zur Berechnung von **105**
trennen **242**
verknüpfen **242**
Verwaltung, Übersicht **241**
View Composer, Verwendung
Aktualisieren von Desktops **231**
Arbeitsblatt zur Erstellung von Linked-Clone-Pools **89**
Auswahl von QuickPrep oder Sysprep **99**
Erstellen von Datenfestplatten **110**
Erstellen von Linked-Clone-Pools **89, 96**
Grundlegendes zu Desktop-Aktualisierungen **232**
Grundlegendes zur Desktop-Neuzusammenstellung **233, 237**
Neuerstellung eines Desktops anhand einer getrennten persistenten Festplatte **244**
Neuverteilung von Linked-Clone-Desktops **238, 240**
Neuzusammenstellen von Linked-Clone-Desktops **234**
QuickPrep **100**
Speichern von Replikaten und verknüpften Klonen in separaten Datenspeichern **109**
Überlegungen zum Speichern von Replikaten in separaten Datenspeichern **109**
Veröffentlichen von Basis-Images **305**
Verwalten von Linked-Clone-Desktops **231**
Vorbereiten einer übergeordneten virtuellen Maschine **75**
Vorbereiten einer übergeordneten virtuellen Maschine für die Neuzusammenstellung **234**
View Connection Server
Ändern des Taktsignalintervalls **327**
Bearbeiten der externen URL **24**
deaktivieren **23**
Dienste **350, 351**
Einstellungen **25**
Entfernen des Eintrags aus der Konfiguration **406**
Exportieren von Konfigurationsdaten **345**
Fehlerbehebung bei Verbindungsproblemen **365, 368**
Festlegen von Gruppennamen **388**
konfigurieren **9**
Konfigurieren direkter Verbindungen **21**
Konfigurieren für die HTTP-Zwischenspeicherung **323**
Planen von Sicherungen **344**
Sammeln von Diagnoseinformationen **364**
Sichern von Konfigurationsdaten **18, 343**
View LDAP-Konfigurationsdaten **25**
Wiederherstellen von Konfigurationsdaten **346**
Zuweisen von Kennzeichen für die eingeschränkte Berechtigung **143**
View Connection Server-Konfiguration, Serverzertifikat **355**
View LDAP
Beschränken der Größe von Basis-Image-Paketdateien **324**
Konfigurationsdaten **25**
pae-mVDIOfflineUpdateFrequency, Attribut **327**
View Transfer Server-Konfiguration
Bestimmen der Größe eines Basis-Images **302**
Entfernen einer Instanz **298**
Festlegen einer maximalen Dateigröße zur Unterteilung von Paketen bei der Veröffentlichung **407**
Festlegen von Replikationsrichtlinien **309**
Grundlegendes zum Transfer Server-Repository **302**
Hinzufügen einer Instanz **297**
Konfigurieren des Repositorys **303**
Konfigurieren von Übertragungsrichtlinien **309**
Optimieren von Datenübertragungen **313**
Sperrung und Entsperrung von Instanzen **409**
Synchronisieren lokaler Desktops **297**
Verbessern der WAN-Leistung **300**
View Transfer Server-Verwaltung
Dienste auf einem View Transfer Server-Host **352**
Migrieren des Repositorys **306**
Statuswerte **300**
Versetzen in Wartungsmodus **299**
Verwalten des Repositorys **302**
View Transfer Server, Fehlerbehebung
Auschecken von Desktops **333**
fehlendes Transfer Server-Repository **337**

Fehler bei Systemzustandsprüfung **337**
Kein Transfer Server-Repository konfiguriert **337**
Pending (Ausstehend), Status **335**
Repository-Verbindungsfehler **336**
Transfer Server-Repository-Konflikt **338**
ungültiges Transfer Server-Repository **336**
Wartungsmodus ausstehend **335**
Webserver nicht aktiv **338**
View-Dienste, starten und beenden **350**
View-Komponenten, warten **343**
ViewPM.adm, ADM-Vorlagendateien **170**
Virtual Printing (Virtuelle Druckfunktion), View Agent, benutzerdefinierte Option **58**
virtuelle Maschinen, Benutzerdefinierte Konfigurationsparameter **52**
Virtuelle Maschinen
Anpassungsfehler **373**
Anzeigen von Informationen **392**
Deaktivieren von Windows 7-Diensten **66**
Desktop-Status **258**
Erstellen von Vorlagen **81**
Installieren des Gastbetriebssystems **54**
verlassen den Bereitstellungsstatus nicht **373**
verwalten **247, 255**
Vorbereiten für die Desktop-Bereitstellung **51, 52**
virtuelle Profile, *, siehe* Persona-Verwaltung
Virtuelle VMware Server-Maschinen, Vorbereiten für die Desktop-Bereitstellung **47**
VMware ThinApp
Integration in View Manager **267**
Verwenden des Setup Capture-Assistenten **269**
VMware Tools, Installieren **55**
VMware View with Local Mode, *, siehe* lokaler Desktop
VMwareVDMDS-Dienst **351**
Vollständig (Nur Lesen), Berechtigung **42**
Volumenaktivierung, Linked-Clone-Desktops **77**
Vorabruf und SuperFetch, deaktivieren **72**
vordefinierte Administratorrollen **27**

W

Wartungsmodus
Anpassen von Desktops **125**
beenden **256**
starten **256**
Starten von Desktops **125**
View Transfer Server **299**
Webkomponente, Dienst **351**
Wiederherstellen, View-Konfigurationsdaten **343, 346**
Windows 7
3D-Rendering **131**
Anpassungsspezifikationen **81**
Deaktivieren der Defragmentierung für verknüpfte Klone **70**
Deaktivieren der Microsoft-Feeds-Synchronisierung **74**
Deaktivieren der Registrierungssicherung **73**
Deaktivieren der Systemwiederherstellung **73**
Deaktivieren des Ruhezustands **78**
Deaktivieren des Windows Update-Dienstes **71**
Deaktivieren des Windows-Diagnoserichtliniendienstes **72**
Deaktivieren von Diensten **66**
Deaktivieren von Vorabruf und SuperFetch **72**
Deaktivieren von Windows Defender **74**
Dienste, die ein Wachstum der Betriebssystemfestplatten verursachen **67**
Volumenaktivierung mit verknüpften Klonen **77**
Vorteile der Deaktivierung von Diensten **66**
Windows Server 2003, Verbessern der WAN-Leistung **300**
Windows Vista
Deaktivieren des Ruhezustands **78**
Volumenaktivierung mit verknüpften Klonen **77**
Windows XP
Deaktivieren des Ruhezustands **78**
Fehlerbehebung bei der GINA-Verkettung **378**
Fehlerbehebung bei verknüpften Klonen, die nicht zur Domäne hinzugefügt werden können **378**
wswc, Befehl
Exitcodes **428**
Konfigurationsdatei **427**
Syntax **425**

X

XML-Ausgabe, vdmadmin, Befehl **383**

Z

Zeigersteuerung in Desktop-Fenster **294**
Zeitüberschreitungslimit, QuickPrep-Anpassungsskripts **80**
Zertifikate
Aktualisieren auf View Connection Server **355**
Probleme ignorieren **174**
Zertifikatssperrliste, Überprüfung
Anmeldung **157**
konfigurieren **157**
Zertifikatssperrüberprüfung
aktivieren **156**
Gruppenrichtlinieneinstellungen **174**

Zwischenspeicherung auf einem Proxy-Server
Bereitstellen lokaler Desktops **323**
einrichten **326**
Zwischenzertifikate
Hinzufügen zu Zwischenzertifizierungsstellen **154**
Siehe auch Zertifikate
Zwischenzertifizierungsstellen, Richtlinie **154**